

in071331

INCITS Study Group on Security Best Practices

Doc No.: SPB07004

Date: 23 August 2007

Project:

Ref. Doc.:

Reply to: SG-SPB, Chair
Edward L. Stull
representing
Direct Computer
Resources, Inc.
20600 Georgia Avenue
Brookeville, MD 208336

Phone: Voice: (301) 260-1781

Fax: (301) 260-1876

Email: estull@datavantage.com

EXECUTIVE BOARD REPORT FOR: INCITS SG-SPB

COVERING THE PERIOD: JULY 2007 TO AUGUST 2007

TITLE OF SUBGROUP: STUDY GROUP ON SECURITY BEST PRACTICES

SUBGROUP'S WEB SITE

SG-SPB uses only the INCITS web site: www.incits.org/tc_home/sbp.htm

1. EXECUTIVE SUMMARY

1.a Informal Description of Work

As specified by the INCITS Executive Board, the Terms of Reference are:

The INCITS Study Group on Security Best Practices will:

- study the security needs and requirements of the financial and insurance services industries and assess what is missing in current standards and practices.
- make a recommendation to the INCITS EB on an approach to create deployable best practices and frameworks for security in these industries. This may include creating Project Proposals for new INCITS Standards or Technical Reports.
- complete its work and submit its report for consideration at the January 2008 INCITS EB meeting.

1.b Overview of This Period

Please see the next section for information about this first period.

The SG-SBP recognizes the extraordinary support of the INCITS Secretariat, in particular the accomplishments of Jennifer Garner and Deborah Spittle, for the critical assistance needed to launch the study group.

2. SIGNIFICANT ACCOMPLISHMENTS

Four of the five officer positions are now filled. Each of the new Vice Chairs are well recognized in their sectors as experts and people of influence. The Secretary position remains open to date.

Membership in the SG-SBP is rapidly changing in that at this writing we are only in the fifth week of formation with the first meeting still about three weeks ahead. The focus of the officers is to first get known expert members from industry and government; this is in progress.

Another focus area of the SG-SBP officers is that of the strategic liaisons and collaboration. As noted later in this report, we are initially seeking relationships (many in progress) with major standards organizations and industry consortia.

Work has begun to form the following Standing Documents:

- SD-1 Document Register (as supported by the INCITS database)
- SD-2 Roles and Responsibilities
- SD-3 Strategic Collaboration (includes liaisons)
- SD-4 Work Plan
- SD-5 Calendar

3. SIGNIFICANT CHALLENGES

Given the intended short lifecycle of the SG-SBP, getting information to the two very large industry sectors of financial services and insurance is paramount but difficult. Nonetheless, this is happening, particularly with the help of the FST Summit (Financial Services Technology Summit) conference to be held in Scottsdale, Az., September 17 – 19. Similarly, getting to the appropriate influential organizations and individuals as well as those with the appropriate expertise is yet another challenge. The officers of the SG-SBP see these challenges best being met through strategic relationships with key standards organizations and industry consortia.

Given the size of the financial services and insurance sectors, reaching a meaningful consensus will also be a challenge. The officers of the SG-SBP see these challenges again being met through the strategic relationships.

Yet another major challenge is the sheer volume of related security activities and documents. This challenge will only be met by acquiring the needed experts, ergo, the reason for this approach being a major focus of the SG-SBP officers.

4. PREVIOUS YEAR'S MEETINGS

None – before the Study Group was organized.

5. ACTIVITIES NEXT YEAR'S MEETINGS

2007 – 2008 PLANNED MEETINGS			
MEETING	DATES	LOCATION	STATUS
1	Sep 19	Scottsdale, Az.	published
2	Oct 4	(telecon)	pending
3	Oct 23	INCITS	pending
4	Nov 20	(telecon)	pending
5	Dec 18	(telecon)	pending
6	Jan 6	(telecon)	pending

6. LIAISON ACTIVITIES

A current area of focus among the SBP officers is that of the strategic liaisons and collaboration. We are initially seeking relationships (many in progress) with major standards organizations and industry consortia:

Liaisons (contact made and in progress, plus more being considered)
AHIP - America's Health Insurance Plans

BITS - not-for-profit, CEO-driven financial service industry consortium
DHS – Department of Homeland Security
FSTC – Financial Services Technology Consortium
INCITS CS1- Cyber Security
INCITS T3 – Open Distributed Processing
NIST – National Institute of Standards and Technology
JTC1 SC27 - IT Security techniques
JTC1 SC7 - Software and Systems Engineering
X9 - Accredited Standards Committee (ASC) X9, Financial Services

7. MEMBERSHIP AND OFFICERS

Membership in the SBP is rapidly changing in that at this writing we are in our fifth week of formation with our first meeting still about three weeks ahead. The focus of the Officers is to first get known expert members from industry and government; this is in progress.

Four of the five officer positions are now filled. Each of the new Vice Chairs are well recognized in their sectors as experts and people of influence. The Secretary position remains open to date.

7.a Officers

Position	Name	Organization
Chair	Edward L. Stull	Direct Computer Resources, Inc.
Vice Chair	Mark G. Clancy	Citigroup
Vice Chair	Robert E. Talbot	Coventry Health Care
Vice Chair	Scott Erkonen	Hotskills, Inc.
Secretary	(vacant)	
Vocabulary	(Not anticipated)	

7.b Membership (pending as of August 2007)

Citigroup
 Coventry Health Care
 Direct Compute Resources, Inc.
 Hotskills, Inc.
 IBM - Tape Drive Firmware

8. FUTURE TRENDS

There is a very strong interest in ICT risk management and compliance. In response, the officers of the SBP, in conjunction with other guest speakers, are conducting a roundtable session at the FST Summit in Scottsdale, Az. on September 18, 2007. Below is the program headliner for that roundtable session:

This lunch-hour session focuses on issues with respect to the policies, practices and deployment of risk management services and controls in the context of compliance requirements and controls. Given competitive pressures, public reactions and profitability goals, a good risk management program entails a strong strategic focus on a business, while accomplished in conjunction, a good compliance program ensures that measures are in place to correctly manage risk within the capacity of that business. Where we are today, where we are going and where we want to be are focus areas in this roundtable discussion.

9. OTHER ADMINISTRATIVE INFORMATION

9.a Administrative Matters of Note

None.

9.b Procedural Matters of Note

None.