The security scenario in the Italian banking sector

Romano Stasi
ABI Lab Market Research Director

Rome 3 November 2005

ISCOM CONFERENCE ON NETWORK AND INFORMATION SECURITY: Political and Technical Challenges
In order to create a network between banks and ICT companies and to address technological evolution towards value creation for the banking sector, **ABI promoted the foundation of**

**ABI Lab Consortium**  
R&D center on technology in banking sector

**What we do:**
- **We collaborate with ABI for the lobbying to public organizations** in order to improve the regulation
- **We develop research activities**, producing analysis and conceptual models applied to banking processes
- **We acquire experience** from case studies and pilot projects
- **We spread the results of our activities** to all our members through different channels (KMS, events, meetings, training, media …)
- **We provide services** to bank and technology partners

120 BANKS  
67 ICT PARTNERS
ICT researching Areas of ABI Lab

**SECURITY**
- Developing an integrated Security model
- Business Continuity solutions of critical processes
- Observatory on Security and Disaster Recovery
- Information sharing of computer threats in the banking sector
- Biometrics and Videorecording systems

**CHANNEL**
- Web ATM
- Observatory on Call Centre in the Banking sector
- Digital Terrestrial Television

**TLC**
- Observatory on broadband in the Banking sector
- Observatory on Mobile technology in the Banking sector

**SUPPORT PROCESSES**
- E-document
- Knowledge Management
- Certified e-mails
- Observatory on corporate portals (INTRANET)
- Banking Processes mapping

Associazione Bancaria Italiana
Security in the banking sector: Costs and investments

**Costs of LOGICAL SECURITY Italy**

(Mln euro)

<table>
<thead>
<tr>
<th>Year</th>
<th>2000</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>105</td>
<td>134</td>
<td>148</td>
<td>190</td>
<td>430</td>
</tr>
</tbody>
</table>

Source: ABI CIPA 2003, 149 banche

**Costs of PHYSICAL SECURITY Italy**

(Mln euro)

<table>
<thead>
<tr>
<th>Year</th>
<th>2000</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Money Transport</td>
<td>243</td>
<td>203</td>
<td>354</td>
<td>215</td>
<td>379</td>
</tr>
<tr>
<td>Theft Protec.</td>
<td>215</td>
<td>153</td>
<td>379</td>
<td>204</td>
<td>357</td>
</tr>
<tr>
<td>Robbery Protec</td>
<td>800</td>
<td>747</td>
<td>833</td>
<td>739</td>
<td>750</td>
</tr>
</tbody>
</table>

Source: OS.Si.F. 2003 (ABI)

**SECURITY INVESTING PRIORITIES**

- Regulatory Compliance
- Reporting and measurement
- Infrastructure Improvement
- Governance
- Security awareness and training

Mandatory requirements are still the main drivers for investing in security.

Logical security is growing constantly compared to physical security.

Source: Deloitte, Security Survey on Financial services, 2005
### Developing Security to mitigate Operational Risks

<table>
<thead>
<tr>
<th>Event Type Category (Level 1)</th>
<th>Definition</th>
<th>Categories (Level 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internal Fraud</td>
<td>Unauthorized activity</td>
<td>Theft and Fraud</td>
</tr>
<tr>
<td>External Fraud</td>
<td>Theft and Fraud</td>
<td>Syndicate Security</td>
</tr>
<tr>
<td>Employment Practices and Workplace Safety</td>
<td>Losses arising from non-compliance with employment, health or safety laws or agreements, from payroll errors, or from employee discipline processes</td>
<td>Employee Relations</td>
</tr>
<tr>
<td>Systems, Products &amp; Business Processes</td>
<td>Losses arising from a natural or social event that results in a material loss to a business process, or from the failure of a business process or system failure</td>
<td>Business Continuity</td>
</tr>
<tr>
<td>Damage to Physical Assets</td>
<td>Losses arising from a natural or social event that results in a material loss to a physical asset, or from the failure of a physical asset or system failure</td>
<td>Business Continuity</td>
</tr>
<tr>
<td>Business Disruption and System Failure</td>
<td>Losses arising from a natural or social event that results in a material loss to a business process, or from the failure of a business process or system failure</td>
<td>Business Continuity</td>
</tr>
</tbody>
</table>

### Op Risk losses are monitored by DIPO an ABI initiative

- Integrated security model
- Business Continuity solution of critical processes
- Disaster Recovery Observatory
- Information sharing of computer threats in the banking sector

Banks are integrating the approach of OpRisks in the Security Processes. Security solutions has to be justified by the reduction of a Operational Risk.

**ABI Lab developing topics regarding Bank Security**
Security scenario: key issues

Establishing a monitoring process to protect ICT Assets

Developing an optimal and integrated Security governance

Focusing Security & Continuity to be on track with compliance scheduling

Business Continuity and Privacy rules are fostering new banks investments in Security

The evolving threats are enforcing the implementation of stable processes to prevent and react on attacks

Key banks are integrating LOGICAL & PHYSICAL SECURITY achieving savings as well as increased protection
Security and compliance in Italy

2005 ICT priorities for the Italian Banking Sector

<table>
<thead>
<tr>
<th>Activity</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basel2 &amp; IAS</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Business Continuity</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Other rules (e.i. 231, 196)</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Enterprise System integration</td>
<td>✔️ ✔️ ✔️</td>
</tr>
<tr>
<td>Branch renewal</td>
<td>✔️</td>
</tr>
<tr>
<td>CRM optimization</td>
<td>✔️ ✔️</td>
</tr>
<tr>
<td>Business Intelligence implementation</td>
<td>✔️ ✔️</td>
</tr>
</tbody>
</table>

• The Italian regulation on PRIVACY appears to be one of the most detailed in the world.

• Italian Banks have been involved in defining the Security Program (DPS) to comply with the regulation.

A BCPlan in every bank by the end of 2006

“Gestione della Continuità operativa” Banca d’Italia July 2004

Source: ABI Lab, Disaster Recovery Observatory 2005, 99 Banks
The business continuity approach is enlarging the traditional security perimeter

- Defining coordination rules to manage the organization during the emergency
- Defining Plans and procedures to guarantee by critical resources and by process
  - Logistic solutions
  - Resource training

Implement Disaster Recovery architecture

- Remote mirrored
- Campus mirroring
- Cold stand-by
- Hot site
- Warm stand-by

Source: ABI Lab, Disaster Recovery Observatory 2005, 99 Banks
After September 11th Central Banks started a process to define measures to be adopted in order to guarantee Business Continuity for the banking system and for a single operator.

2002: Kick-off activities

July 2004: Rules on “Business Continuity Management” for banks;

November 2004: “Guidelines for service continuity of qualified payment systems infrastructures”.

2003-2006: Defining a BCP (including tests) at system level to coordinate the key banking operators and to guarantee vital services

Participating in the activities of Banca d’Italia;

Collaboration with third parties and critical national infrastructures;

2004 Methodology for developing a Business Continuity Plan;

2005-2006 Developing a deep understanding on BC solution & technologies for critical processes
The first objective has been achieved developing a Methodology to comply correctly with the principles of Banca d’Italia by the end of 2006.
ABI Lab has developed a training system to increase Business Continuity competences in the banking sector and to help banks on implementing the methodological phases.

Banks participating on ABI Lab BC Training

More than 14500 trained man/hours during last year
Security scenario: key issues

- Focusing Security & Continuity to be on track with compliance scheduling
- Establishing a monitoring process to protect ICT Assets
- Developing an optimal and integrated Security governance
- Business Continuity and Privacy rules are fostering banks on new investments in Security
- The evolving threats are enforcing the implementation of stable processes to prevent and to react on attacks
- Key banks are integrating LOGICAL & PHYSICAL SECURITY achieving savings as well as increased protection
Monitoring identity theft and phishing

Phishing attacks detected in Italy

- The total number of phishing attacks detected in Italy is still very low (30) compared with US scenario (~14000 per month).

- In the last two months, an increase in number as well as in technological sophistication have raised the attention among Italian banks (see for example the production of password stealing malicious software).

Ref: ABI Lab, Centrale d’allarme per attacchi informatici, 2005

Ref: Anti-Phishing Working Group, Phishing Activity Trends Report - July 2005
Identity Theft: an ubiquitous threat

Identity theft can be traced upon the whole identity processing. The threats equally attack banks and customers, as well as the connection between them. **ABI Lab has disseminated a Decalogue** for banks and customer to reduce the risk of identity theft and phishing.
Integrating channels to protect accesses

The number of different bank channels providing services requires a new focus on technological and organizational solutions to manage correctly customer identity.
Security scenario: key issues

Establishing a monitoring process to protect ICT Assets

Focusing Security & Continuity to be on track with compliance scheduling

Business Continuity and Privacy rules are fostering banks on new investments in Security

The evolving threats are enforcing the implementation of stable processes to prevent and react on attacks

Key banks are integrating LOGICAL & PHYSICAL SECURITY achieving savings as well as increased protection

Developing an optimal and integrated Security governance
Evolving the security governance

The risk management drives the implementation of a new model for the banking security management. Starting from risky events and business impacts, the banks are defining a new cross-functional governance and an integrated security infrastructure.