Changing Landscape of Financial Intermediation

Cyber security in finance

John Trundle
CEO, Euroclear UK & Ireland
Washington, 4 June 2015
Cyber risks in perspective for financial market entities

- Critical dependency on IT systems (esp. FMI's)
- More than an IT issue – a business issue
- How to assess threats and vulnerabilities
- Managing risks – IT architecture, monitoring, hygiene, people
- “What if?” planning
Dependencies and responsibilities

- Use of IT - reliability, volume, STP
  - efficiency & risk reduction
  - but dependency → op risk (including cyber)

- Easy to believe threats are for technicians (fast changing, complex)

- Business issue too; for financial market entities and their regulators

- Staff need to be aware; good “hygiene” provides a lot of resilience

- Identify key business services and relevant threats and vulnerabilities, including inter-dependencies.
Managing risks

Good IT (prevention)
- architecture (hard to maintain “coconut” model)
- controlled limited external access
- patching promptly; anti-virus software
- password and access control (complexity, change)

Hygiene
- in IT, but also day to day
- office security, badges

Monitoring (detection)
- Internal traffic and variations; audit trails
- penetration testing
- alerts, CIRT (info sharing), threats continuously evolving

People
- culture, alertness
- staff training (phishing etc)

Response
- identification of type of incidents; escalation; communication; appropriate action
What if?

- Business continuity exercises (technical, business responses)
- Potentially different responses (operational stability v. security)
- Do practice exercises internally and market wide
Key messages

• Not just an IT issue
• Get basics right – provides good first level of resilience
• Ensure staff understand risks and are alert
• Follow evolving best practice, share information and monitor systems & threats
• Plan for the worst
## Annex: Some components of a cyber risks plan for financial institutions

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>business involvement (boards, Audit and Risk committees)</td>
</tr>
<tr>
<td>Threat management</td>
<td>info exchanges</td>
</tr>
<tr>
<td>Cyber attack plan</td>
<td>phishing tests</td>
</tr>
<tr>
<td>Development cycle</td>
<td>cyber threats integrated in application testing</td>
</tr>
<tr>
<td>Network profiling</td>
<td>analytics (what is normal?)</td>
</tr>
<tr>
<td>Brand effect</td>
<td>scan social media for threats and social engineering</td>
</tr>
<tr>
<td>Data monitoring</td>
<td>how is data moved and stored normally?</td>
</tr>
<tr>
<td>Profiling</td>
<td>risks associated with customers, staff, geographies</td>
</tr>
<tr>
<td>Business recovery planning</td>
<td>desk top and live play exercises</td>
</tr>
</tbody>
</table>
Post-trade made easy