Financial Sector Cybersecurity: who’s in charge?

Aquiles A. Almansi
Lead Financial Sector Specialist WBG-Finance & Markets
Issues in the Governance of Central Banks (BIS 2009)
Are cyber risks special today?
Cyber threats, a growing systemic risk (BIS 2014)

1. The role of technology in the provision of financial services has deepened;
2. The degree of interdependency and interconnectedness between operators in financial markets is very high and growing;
3. Both attackers and their motivations have become more diverse, bringing fresh threats from unexpected sources. Attackers now include “hacktivists”, who seek merely to disrupt activity; cyber criminals motivated by financial gain; terrorists aiming to cause political and financial instability; and nation state-related actors attempting to interfere with or gain access to sensitive information, or to cause systemic instability

Committee on Payments and Market Infrastructures (November 2014)
Incidents 2014

DATA RECORDS STOLEN/LOST BY INDUSTRY 2014 YEAR IN REVIEW

Source: Gemalto/SafeNet
## Selected Incidents 2014

<table>
<thead>
<tr>
<th>Organization</th>
<th>Records</th>
<th>Industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Depot</td>
<td>109,000,000</td>
<td>Retail</td>
</tr>
<tr>
<td>J P Morgan Chase</td>
<td>83,000,000</td>
<td>Financial</td>
</tr>
<tr>
<td>Ali Express</td>
<td>300,000,000</td>
<td>Retail</td>
</tr>
<tr>
<td>Korea Credit Bureau, NH Nonghyup Card, Lotte Card, KB Koomin Card</td>
<td>104,000,000</td>
<td>Financial</td>
</tr>
</tbody>
</table>
Who should be in charge?

“IT strategy being a part of corporate strategy, should be driven by the board. All the aspects of technology management, namely, cost, human capital, hardware and software, vendors and service providers, risk management including disaster recovery should be factored in the IT strategy of the bank. The Chief Information Officer (CIO) in a bank needs to work in close coordination with business, finance and legal departments as well as with other user groups within the bank.”

Harun R Khan, Deputy Governor of the Reserve Bank of India
28 July 2015
What have we (WBG-F&M) observed?

Sources:

• Results of recent survey on cyber-security awareness and preparedness among 14 central banks in Eastern Europe (http://www.worldbank.org/en/events/2015/05/18/cyber-preparedness-seminar).

• Behaviors observed in recent simulations run in Eastern Europe, Latin America, North and South Saharan Africa, and East Asia.
Survey: info on incidents

- Eleven of the fourteen respondents acknowledged to have been targets of cyber-attacks.

- Knowledge about cyber-attack attempts and successful breach incidents of financial institutions in their respective jurisdictions varies considerably across the fourteen countries. No information in five of them.

- Ten of fourteen respondents reported to have no information about cyber-attacks to major utility providers, retail stores, or other public or private institutions holding customer bank or credit card data.
Survey: self assessments

- The strongest self-assessments correspond to technical issues typically in charge of IT departments: networks segmented into multiple trust zones, security software automatically updated, etc.

- The weakest self-assessments correspond to areas typically in the hands of Senior Management and/or the Governor/Board: no cyber security awareness training required from supervised institutions, no regular cyber-attack and recovery simulation exercises, no external communication plan to address cyber security incidents, no regular testing with third party cyber-risk mitigating services, etc., etc., etc.
Crisis Simulation Exercises

➢ WBG-F&M has offered more than 30 financial crisis simulation exercises since 2008: “war games” for Ministers of Finance, Central Bank Governors, Heads of Bank Supervision, and other senior officials from national financial sector authorities.

➢ Our more recent crisis scenarios frequently involve cyber incidents, from extended disruption of ATM networks to the spread of malware. The typical responses are, unfortunately, fully consistent with the self assessments.
From: Beta Bank CEO
To: Bank Supervision
Subject: Preliminary forensic report

We have received a preliminary report from the forensic analysis of the strange phenomenon affecting our ATM network, which has already accumulated around 923,000 euros in unauthorized cash withdrawals. The diagnostic is truly worrisome: the forensic lab has found a new, so far unknown ("Zero Day") variant of the malware attributed to the "Carbanak" gang (which, according to press reports, has been behind cyber-attacks to more than 100 financial institutions in 30 countries over the last two years). If confirmed, this would have two very serious practical implications: 1) our infected IT system could be under absolute control of the gang, which having acquired administrative rights could be in position to not only keep extracting cash from the ATM network, but also to make unauthorized transfers, modify or even destroy our records, etc., and 2) any other institution regularly corresponding with us over the last two years via email, or any other electronic means, could potentially have also been infected by the malware, consequently being exposed to similar threats.

The forensic lab has provided the attached CarbanakDetector.exe program, which can be used to verify if Windows machines are infected with this malware. If when running this program Windows does not recognize it as executable, the machine is infected.
Email copied below contained a virus in the attached file that we have deleted. It is our opinion that our IT system is also infected. Please be aware that we will not send further e-mails until we have confirmation from the IT Dept that the Central Bank’s email system is secured.

-----Original Message-----
>>>From: Beta Bank CEO
>>>To: Bank Supervision
>>>Subject: Preliminary forensic report

>>>We have received a preliminary report from the forensic analysis of the strange phenomenon affecting our ATM network, which has already accumulated around 923,000 euros in unauthorized cash withdrawals..........
Group Discussion

- Is cybersecurity a major concern in your jurisdiction? Why? Why not?
- Who leads cybersecurity preparedness in your institutions?
- What is being done right and what remains to be done?
- Is there a formal mechanism to share information on cyber incidents in the financial sector, and in non-financial organizations holding substantial amounts of bank data?
Thank you!

aalmansi@worldbank.org