Privacy, Identity and Information Sharing: Risks and Opportunities

Jeremy Grant

Managing Director

The Chertoff Group

THE CHERTOFF GROUP

WORLD BANK GROUP

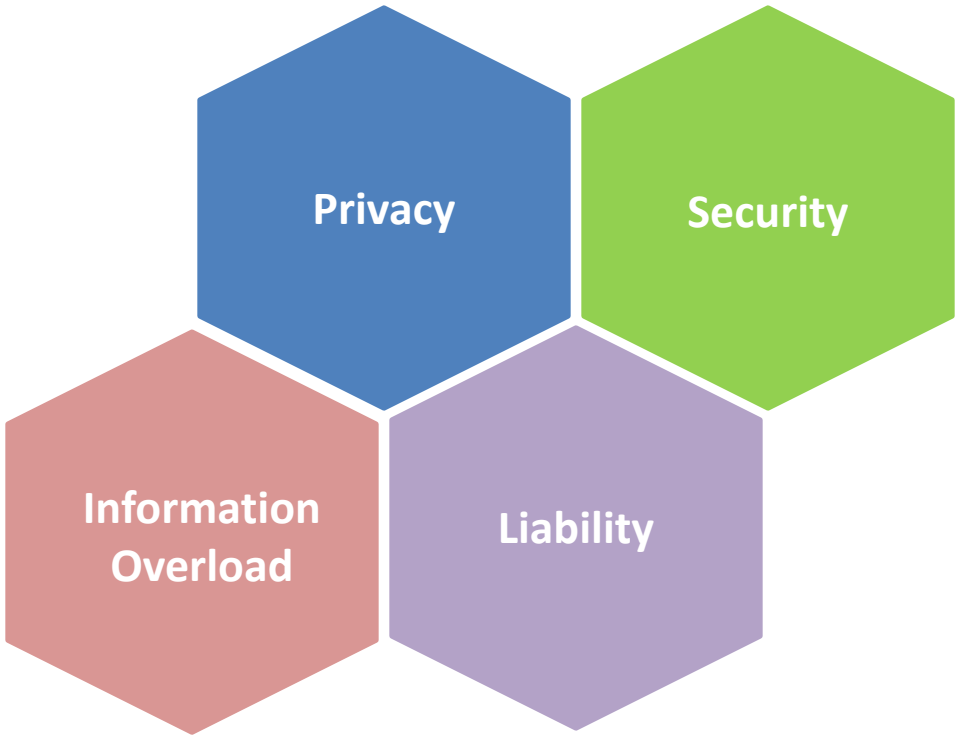
OASIS

Opening Thoughts

- Addressing many modern cybersecurity challenges requires collaboration
  - Between private sector entities – sometimes in the same country, sometimes in multiple countries
  - Between private entities and government (or governments)
  - Between multiple governments

Collaboration Offers Many Benefits…

…And Collaboration Creates Concerns



Liability

- Could reliance on incorrect data result in significant losses due to fraud and/or render an entity liable?
- Is there a construct to ensure information shared is done in accordance with regulatory restrictions?
  - How does this work across borders?
- What liability might parties face if they mishandle data that is collected?
- What redress is there for consumers who think their data may have been misused?

Privacy

- How much data do parties collect that can be tied to individuals (or groups of individuals)?
- What is done with that data? How is it stored? Analyzed? Resold?
- Can information be “anonymized” so that relevant elements can be shared without including PII?
- Is there a broader set of “digital exhaust” in the metadata that is left behind, and that may enable additional tracking and identification? How is data aggregated or linked across transactions?

Note:

This is not an “IT problem”

Core Questions

- How do you enable collaboration – both on a technical and policy level—to get the benefits without creating new privacy or security concerns (or legal)?
- How do you handle this across borders? What new issues does international collaboration create? How can you effectively address them?

Conflicting institutional commitments: what to do about them?

Aquiles A. Almansi

Lead Financial Sector Specialist

WBG-F&M

WORLD BANK GROUP

OASIS

What do we (WBG-F&M) see?

Our sources of information:

- A recent survey among 15 Eastern European Central Banks .
- Several financial-crisis simulation exercises in Eastern Europe, Latin America, North and South Saharan Africa, East Asia.

Survey: info on incidents

- Eleven of the fourteen respondents acknowledge 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

- We at WBG-F&M have 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.

What to do?

Our practical problem is to find ways of convincing financial sector authorities in our client countries that:

- Cyber-risk has become “the” source of “operational risk” in their systems.
- Cyber-risk is not just a technical issue, to be left exclusively in the hands of the “IT guys”. User behavior is an essential aspect of it.
- Cyber-risk is potentially systemic, and to timely inform and be informed about incidents happening anywhere, can prevent a major disruption.

Thanks!

aalmansi@worldbank.org

WORLD BANK GROUP

OASIS

Calibrating Information Sharing Collaboration

Joseph Lorenzo Hall

Chief Technologist

Center for Democracy & Technology

CENTER FOR DEMOCRACY & TECHNOLOGY

WORLD BANK GROUP

OASIS

Adversarial Collaboration?

- Governments both regulate/enforce laws against businesses *and* provide cybersecurity support and infrastructure.
- Different sectors are tolerant of different levels of collaboration, just as they are different levels of regulation and enforcement.
- Seen generally, information sharing must be *carefully* calibrated *adversarial* collaboration

Adversarial Collaboration!

- Human rights and civil liberties benefit from arms-length relationships
  - NSA/GCHQ/&c regularly attack some customers
  - Business relationships are not immune
- Different across sectors: tech vs. finance
- Substantial risk: relationships that are too cozy
  - E.g. US use of informal requests for phone records

Maintaining Roles

- There must be mechanisms on both sides to ensure relationships are not too comfortable.
  - On the business side, record keeping and decisions-to-share must be done carefully
  - On the Gov side, robust oversight and recognize when sharing is not necessary
  - There are always exceptions… (exigency)
- From my research, suspect much is mindset

Calibrate What to Share

- Only share what collaborators need and and can practically use
  - Only largest businesses can chomp on raw data.
  - Most need *actionable* data sharing (sigs, lists, etc.) and trustworthy analytical products
- Liability is actually a good thing!
  - Blanket limitations will do more harm than good

Privacy vs. Security?

- For both business and government:
  - Don't take the security side as a given
  - "User-centered information sharing and intel": understands risks of undermining trust
- For civil society, users, the public
  - Privacy must yield for certain good to be realized
  - Appropriate security controls can undermine "big brother" slippage and improve security of society

SAFE-BioPharma – ETSI Digital Signature and eID Alignment Update

Peter Alterman, Ph.D.

Chief Operating Officer, SAFE-BioPharma Association

WORLD BANK GROUP

OASIS

Rationale for Aligning Trust Policy Frameworks

- There needs to be a common trust framework amongst governments so they can exchange signed digital files that are recognized by each other for international G to G and also in the murky world of healthcare where the distinction between G to G and B to B blurs.
- Imagine a 70 year old US citizen being hit by a bus while visiting Spain where access to his EMRs is critical and where digitally signed electronic hospital bills, treatment documents, lab tests, etc. will be submitted to his insurer and Medicare when he returns home.
- In the biopharmaceutical space, we need Qualified certificates to be recognized by USG regulators when some of our member companies submit digitally signed electronic documents to FDA, DEA and USDA and vice versa, when some of our member companies submit electronic documents to the European Medicines Agency using certificates from US CAs cross-certified with SBCA/FBCA.

SBCA-ETSI Alignment: General Background

- 2014: European Parliament passes eIDAS regulation, requiring revamping of ETSI
- 2014: Riccardo Genghini meets SBP and urges us to help align US and EU digital policies
- 2015: SBP maps Bridge CA Policy to emerging ETSI standards for Qualified digital signatures and eID
- 2015: SBP presents results to ETSI Workshop in Sophia-Antipolis, France and proposes joint alignment effort
- 2015: ETSI Work Group takes up SBP mapping
- 2015: SBP accepts ETSI invitation to membership

SBCA-EU Alignment: Current Status

- Summer 2015: ETSI Work group reviews SBP results; finds no additional areas of discontinuity
- Summer 2015: SPB reviews comments and provides responses
- Summer 2015: Requests for cross-certification with SBCA from a Spanish Qualified CA, European Bridge CA in Germany (commercial); inquiries from others
- September 2015: SBP-ETSI joint work group meets to complete revision to ETSI standards in harmony with SBCA CP
- October 2015: EC votes on adopting revised ETSI QCP standards
- October 2015: ETSI Board votes on SBP membership
- November 2015: ETSI + SBP work group takes up other services, e.g., encryption, time stamping, etc.

#BorderlessCyber

Questions ?