FinTech: The Threat Landscape and Promising Initiatives

Information Security Conference for the Financial Sector

Doha, Qatar

5 November 2017

The FinTech landscape

- In the first nine months of 2016, global investment in FinTech reached 21 billion USD
- New investment has propelled innovation, which is revolutionizing the FinTech sector
- Just as FinTech continues to evolve, so too does the threat landscape and the stakes involved with not employing cybersecurity measures

(Financial Stability Board, 2016)

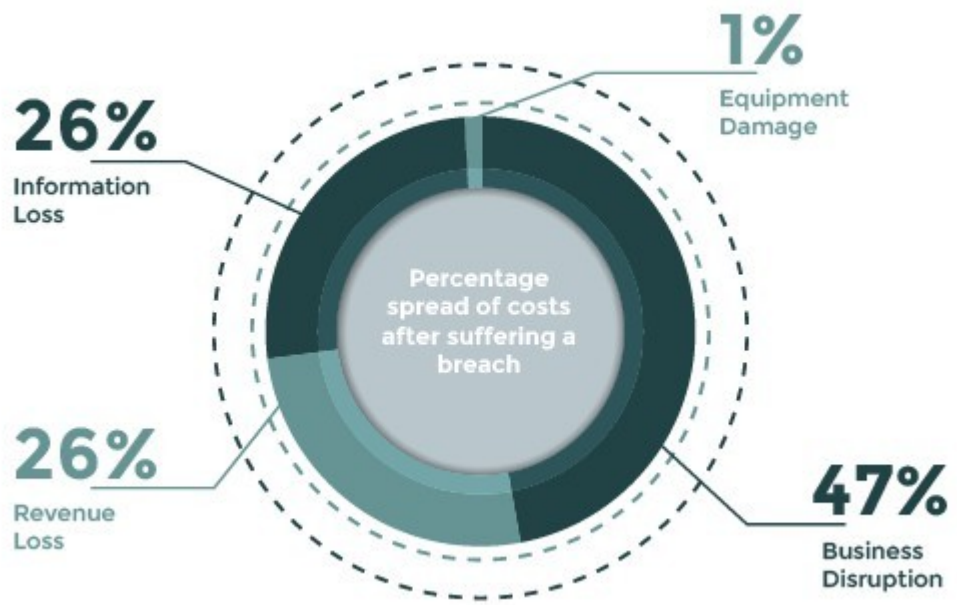
Costs of FinTech Cyberattacks

Costs of cyberattacks

- The costs of not employing sound cybersecurity measures can be accrued in the following ways:
  - **Direct costs:** the actual monetary values
  - **Indirect costs:** the amount of time, effort, and other organizational resources devoted to cyberattack resolutions
  - **Opportunity costs:** the lost business opportunities as a consequence of negative reputation, which usually occurs after the attack is publicly reported, including to victims

Costs of cyberattacks

- According to the Ponemon Institute, companies incurred the following direct costs after suffering a cybersecurity breach:



Possible Threats

Types of cybersecurity threats

1. **Loss of financial data:** Financial data breaches are on the rise due to lack of data encryption for sensitive data
2. **Internet of things and cloud computing weaknesses:** Easily hacked by cybercriminals
3. **Third-party financial services:** Some of the services provided by third parties to financial institutions may be prone to cyber-attacks

Types of cybersecurity threats

5. **Risks of mobile banking:** More and more people are conducting banking transactions on their mobile phone. However, sensitive data stored on your mobile device is at a huge risk

6. **Manipulation/Alteration of Data:** Hackers intentionally change or manipulate the user/organization's data, in order to compromise it

7. **Malware threats**: The popularity of 'Bring Your Own Device' (BYOD) increases the opportunity of affected devices being present over the connected network. Hidden malware in one device can then hijack customer data from devices easily

Types of cybersecurity threats

8.Sophisticated spoofing attacks: Hackers can hijack your bank's website and steal user-related data

9.Chip/PIN attacks: attacker can capture what is called Track 2 data that's transmitted from the card to the card reader using a small Raspberry Pi computer. The captured data, which is sent unencrypted, can then be used to create a normal magstripe card for use on older, offline systems

10.ATM cyber-attacks: Massive financial losses to be incurred by such attacks

Possible Risks

What are the potential risks?

National legal and regulatory risks

Under-resourced and unskilled personnel

Risks in market behaviour

Cyber-threats

Macro-financial risks

Cross-border legal issues

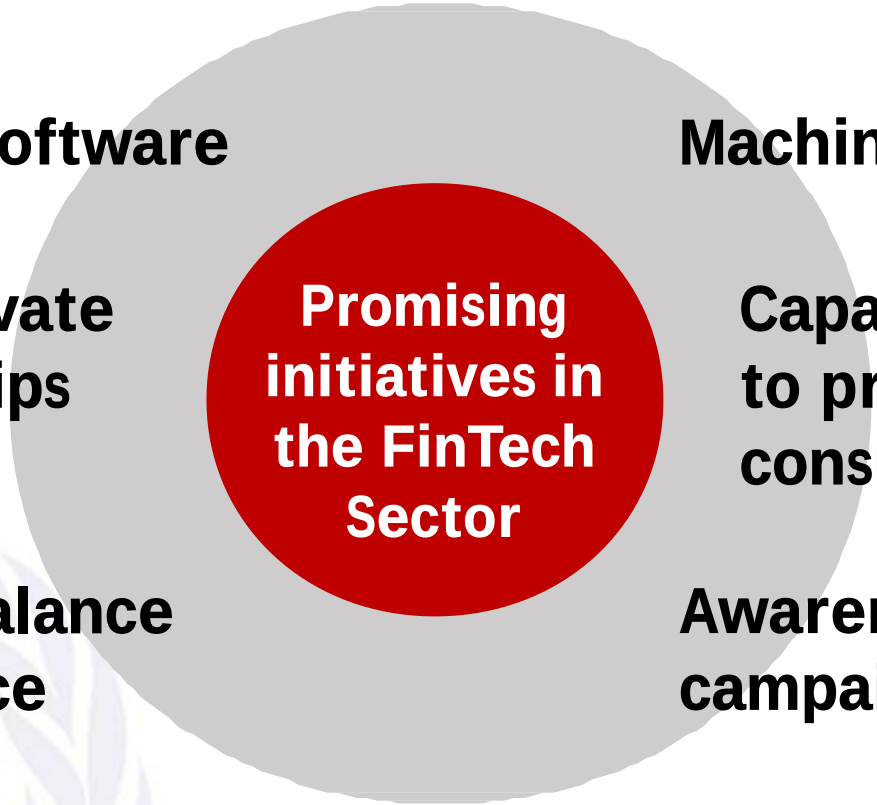
Further potential risks?

Rapid innovations

Third party reliance

Promising Initiatives

Advancing cybersecurity



Compliance software

Machine learning

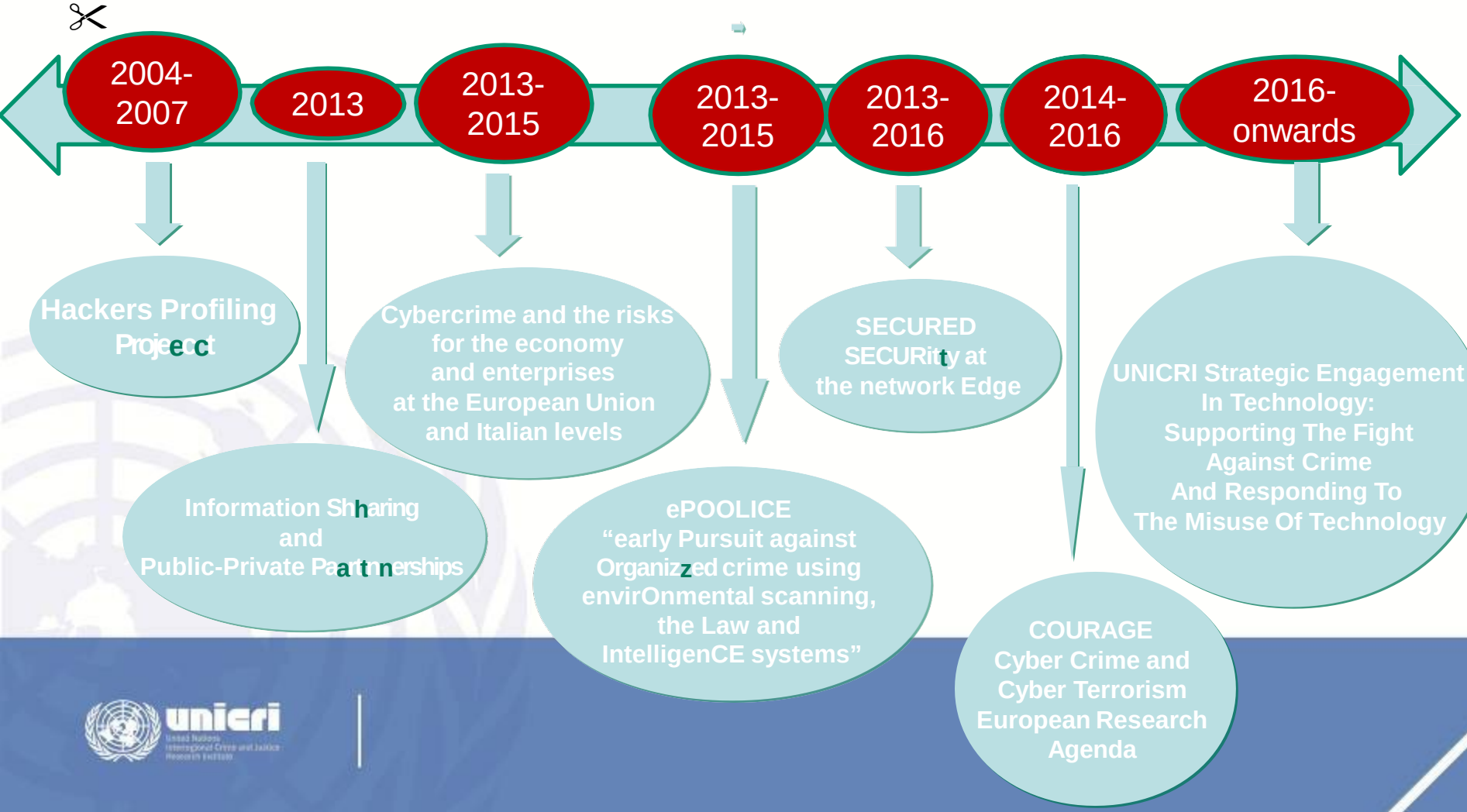
Public-private partnerships

Capacity-building to protect consumer data

Regulatory balance and coherence

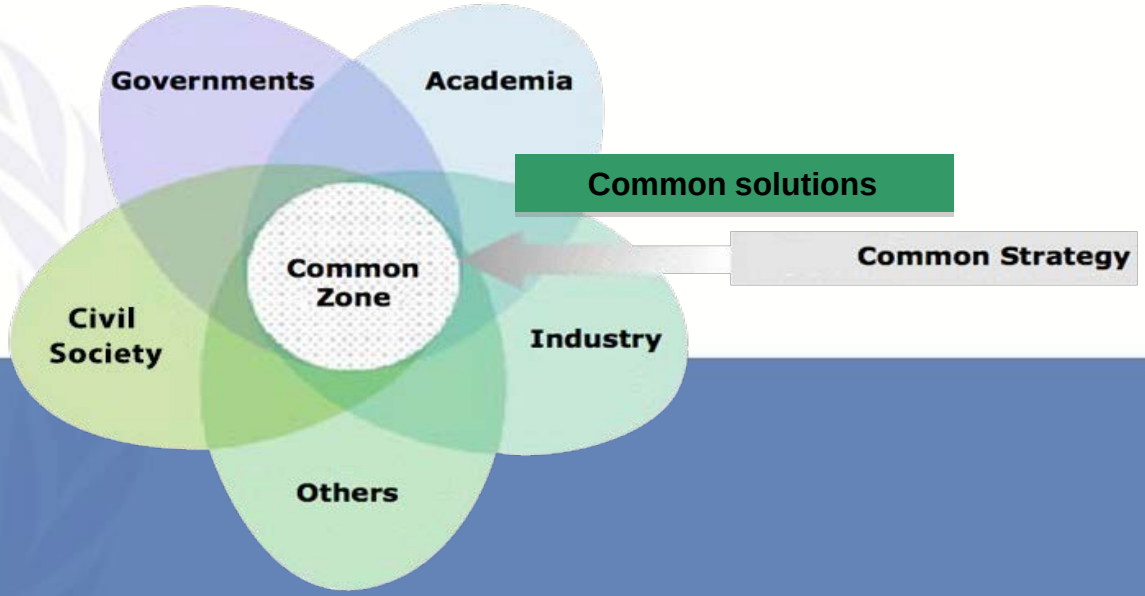
Awareness raising campaigns

UNICRI Cybersecurity and Technology Misuse



Current UNICRI initiative: SIRIO-Security Improvements through Research, Technology and Innovation

- Analyse emerging and future security risks;
- Identify emerging technology to match security needs;
- Promote the use of technology based-solutions to increase security;
- Raise awareness and inform policy-makers about risks and solutions.



Francesca Bosco
UNICRI Programme Officer

bosco@unicri.it

Twitter @francibosco