Cybersecurity and Cybercrime in a Complex World

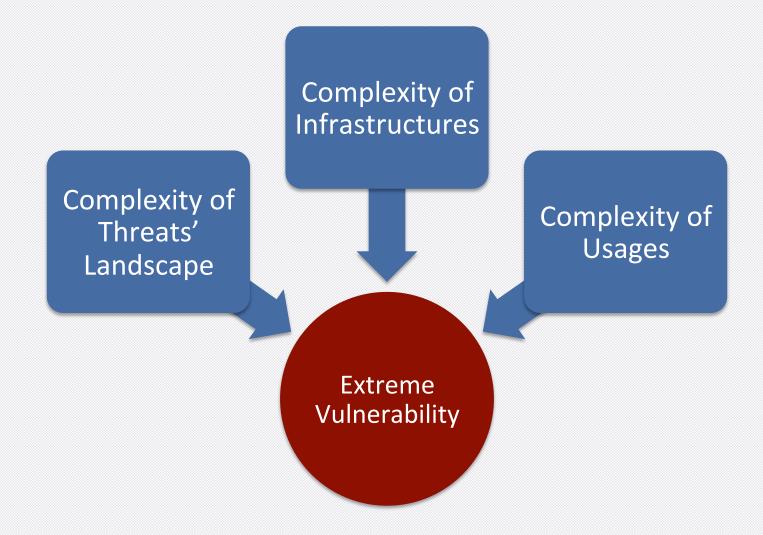
Global Forum

Geneva - 17th Nov. 2014

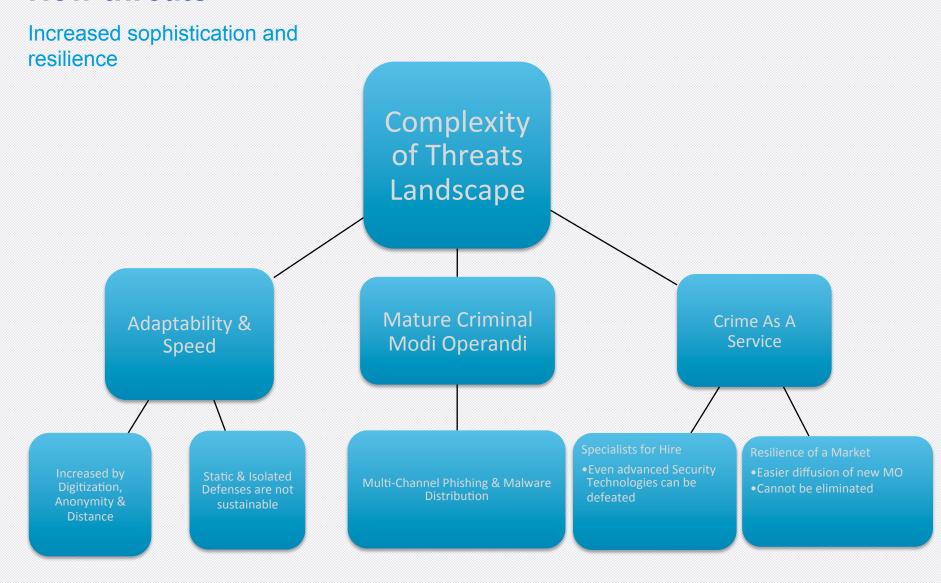


Growing challenge to security

Facing Complexity



New threats



Explosive growth of infrastructures

One Device, Many Users

> Kiosk, POS, X-Box, domestic appliances (TV)...

One User, Many Devices

> **BYOD & Shared** usage => Device **Profiling more** complex to achieve

Several Transactions from different origins, but legitimate

Mobile & New Access Methods

"Cheap Smartphones"?

- Robust design?
- Can they be identified?

Is the underlying Network Safe?

What about Mesh?

Virtualization and **Platforms**

> How to handle reputation?

Where does the user come from?

Is it still possible to blacklist IPs'? (Telcos' NAT)

Innovation in usages feeds complexity

Smoother and more interactive usage

- Through Rich and Dynamic Interfaces, with Client-side processing
- Simplicity and ease of use

Greater Choice

• Thanks to Platformization & Apps' Markets

Use On the Go

- Requires Mobile Platforms
- UI Limitations

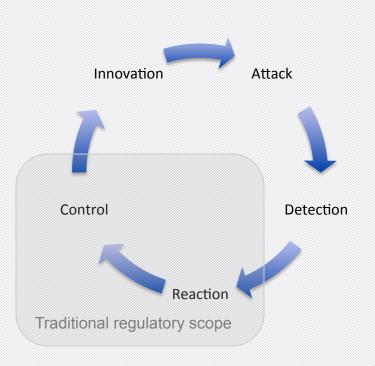
Social Networking

• Disclose Personal Details and facilitate impersonation / Social Engineering

ANYWHERE - ANY WAY - ANY TIME

Can cybersecurity be regulated?

The pace of traditional regulatory mechanisms is too slow



A timeframe expressed in years

- > "Detection" occurs only when the volume of attacks is meaningful.
- "Reaction" is out of scope. Analysis takes time to form consensus.
- "Control" may happen after years, when regulations are implemented.
- > Fraudsters adaptation cycle is far faster : mostly results based.

Towards smart regulations for cyber security matters

Regulators promoting a fast-paced adaptation of the industry

Inclusive	Business interest of industry – Incumbents and disruptors		
	Right and benefits of end-users		
	Obligations and needs of governments		-
Data intensive	Give more scientific ground to best practices	– Act	Observe
	Allow for acceptance and innovation	1	
	Shorten the decision cycle	-	
Outcomes focused	Result is more important than the chosen technology to deliver it.	Decide	Orient
	Open the way to a continuum of incentives.		
	Sensemaking		

Conclusion

Security on Internet is challenging, but not impossible

- Security has to keep pace with technology, innovation, emerging needs and usages of end-users, but also sophistication of attackers → Agility and Robustness
- Security has to take advantage of, and promote a diverse ecosystem to prevent and disrupt massive and automated attacks.
- Security has to be flexible and non-intrusive, as the real added-value is in the protected service, which should not be disrupted.
- Security needs active participation of every stakeholder. In particular, industry should think beyond the perimeter, and regulators have to embrace smart regulatory practices to help stakeholders stay focused on actual outcomes.

The result should be a more secure internet able to evolve along with the pace of innovation while handling its growing complexity

Thank you for your attention

