CEMLA-FIGI Financial Sector
Cyber Resilience Workshop

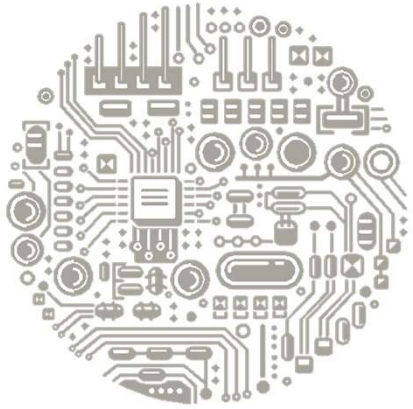
Cyber Resilience - Building Trust Through Public Private Partnerships

Martin Boer, Director

Regulatory Affairs Department

Financial sector perspectives on resilience

- Current threat landscape
- How the industry is responding
- The emerging regulatory response
- Building partnerships around resilience



Cyber Attacks Are Growing Rapidly

- Cyber attacks are increasing rapidly in number, intensity and sophistication.
- The Marriott Attack (2018) exposed 500 million users accounts. Yahoo – largest ever – recalculated to affect 3 billion users
- Also Equifax, WannaCry, NotPetya, etc.
- Cybercrime costs include damage and destruction of data, stolen money, lost productivity, disruption of business, financial markets, reputational harm, and a broader loss of confidence.
- The financial sector has traditionally been the largest target, due to both the money and the data at stake.

- **Annual global cost of cyber events is estimated to rise to USD 6 trillion by 2021, from USD 400 billion in 2015.**

Perpetrators Constantly Evolving

Motivated by

- Thrills
- Challenge
- Financial gain
- Commercial gains
- Espionage
- Political agenda
- Warfare

The rise of nation state-sponsored attacks is difficult for industry alone to address – and necessitates public-private sector collaboration.

Increased CRO Focus on Cybersecurity Risk

Top priority for CROs (10th IIF/EY Global Bank Risk Management Report – 2019)

	CRO priorities 2012—2019							
Rank	2012	2013	2014	2015	2016	2017	2018	2019
1	CRE	CRE	CRE	REG	REG	CY	CY	CY
2	LIQ	RA	RA	RA	CY	REG	CRE	CRE
3	RA	REG	OR	CRE	CRE	CON	REG	DIG
4	MR	OR	REG	OR	RA	CRE	OR	CON
5	REG	LIQ	RC	CAP	OR	OR	TECH	REG
6	TECH	CAP	CAP	LIQ	TECH	CUL	CON	OR
7	STR	MR	MR	TECH	STR	TECH	RA	CUL
8	CAP	STR	LIQ	STR	CON	ERM	BM	PRI
9	RC	TECH	STR	MR	CUL	RA	CUL	RES
10	OR	RC	TECH	CY	ERM	STR	STR	MO

Key	
Financial risks	
CAP	Regulatory capital management
CRE	Credit
LIQ	Liquidity
MR	Market risk
MO	Model
REG	Regulatory implementation
STR	Stress testing
Nonfinancial risks	
BM	Business model
COM	Compliance
CON	Conduct
CUL	Culture
CY	Cybersecurity
PRI	Data privacy
ERM	Enterprise risk management
OR	Operational
RES	Operational resilience
REP	Reputation
RA	Risk appetite
RC	Risk controls
TECH	Risk technology architecture
DIG	Transition to digital

Increased Board Focus on Cybersecurity Risk

Top priority for Boards (10th IIF/EY Global Bank Risk Management Report – 2019)

	Board priorities 2013—2019*						
Rank	2013	2014	2015	2016	2017	2018	2019
1	RA	RA	COM	REG	CY	CY	CY
2	LIQ	COM	RA	CY	REG	REG	CRE
3	REG	LIQ	CRE	RA	BM	RA	DIG
4	CAP	CAP	LIQ	CUL	RA	CRE	CON
5	OR	OR	CUL	CRE	CRE	CON	REG
6	STR	STR	CON	CON	CUL	OR	CUL
7	ERM	REP	OR	CAP	CON	BM	OR
8	CUL	CON	CAP	STR	REP	REP	BM
9	TECH	CUL	TECH	OR	OR	CUL	RES
10	REP	ERM	STR	TECH	STR	CAP	RA

Key	
Financial risks	
CAP	Regulatory capital management
CRE	Credit
LIQ	Liquidity
MR	Market risk
MO	Model
REG	Regulatory implementation
STR	Stress testing
Nonfinancial risks	
BM	Business model
COM	Compliance
CON	Conduct
CUL	Culture
CY	Cybersecurity
PRI	Data privacy
ERM	Enterprise risk management
OR	Operational
RES	Operational resilience
REP	Reputation
RA	Risk appetite
RC	Risk controls
TECH	Risk technology architecture
DIG	Transition to digital

* CROs' views of boards' priorities

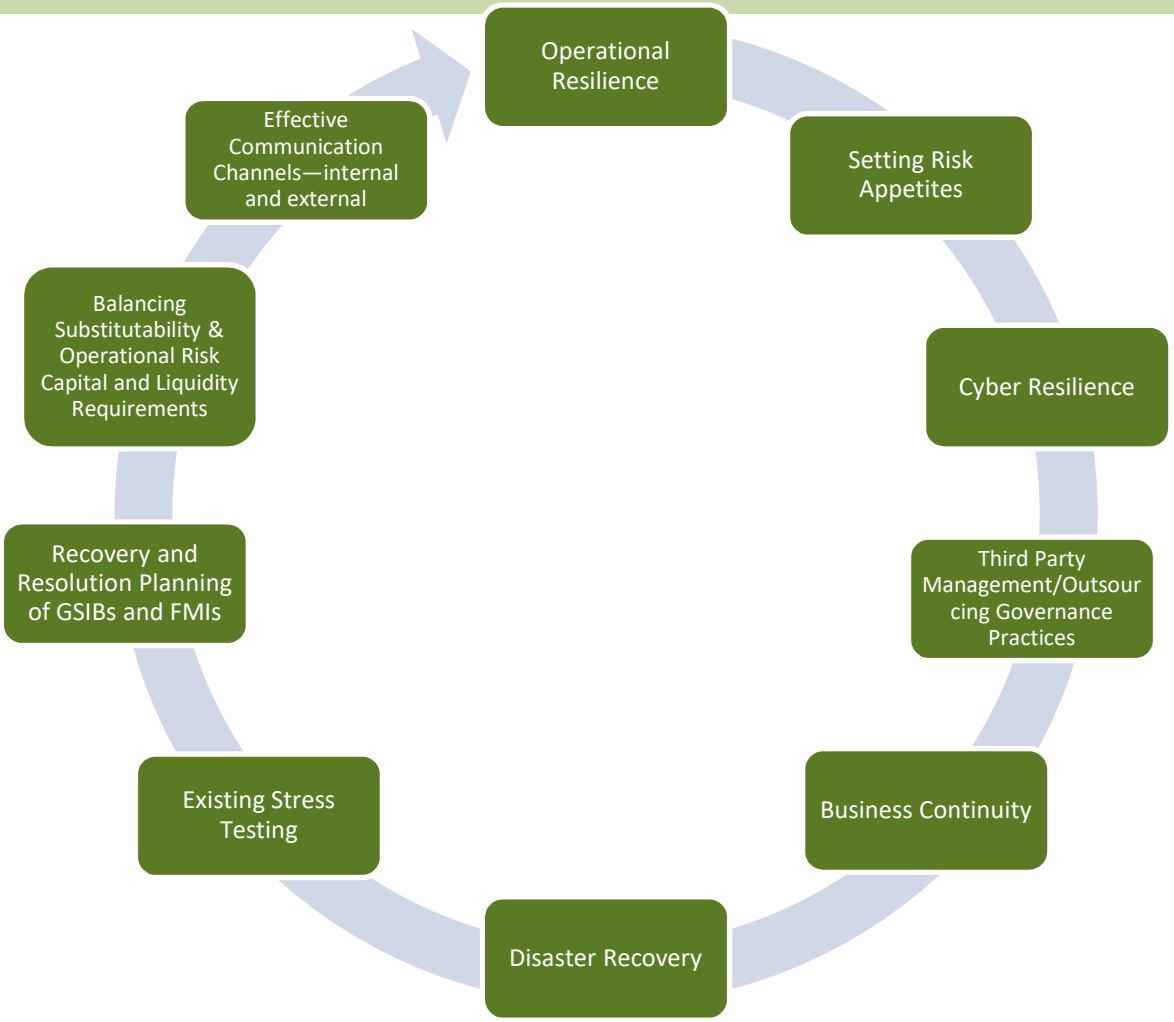
Financial Industry approach to Cyber

Holistic enterprise approach to Cyber Resilience:

- Role of Chief information security officer (CISO)
- Large Cyber/IT budgets
- Investment in control functions
- Safeguarding critical data
- Risk management, as non-financial Risk
- Industry-wide information sharing platforms
- Working together with government and law enforcement

Enterprise-wide focus on Operational Resilience

Knitting together multiple existing financial sector disciplines…..



Challenges for Financial Services firms

- Fast-evolving environment, threat escalation
- Talent issues – lack of skilled Cyber experts
- Limitations around usage of data
- Role of third party vendors (concentration of cloud providers)
- Increased regulatory fragmentation

Transmission Channels for Cyber Risk

Different channels that can impact financial stability

Regulatory Fragmentation around Cyber Risk

- Understandably, authorities around the world have developed strategic initiatives, guidance papers, regulatory and supervisory approaches, aimed at strengthening the resilience of institutions and the financial system.

- Cyber-attacks rarely happen within national borders, therefore it should be avoided that weak-links form in jurisdictions or industries, including new entrants, where lower standards might apply, posing risks to others in the global financial ecosystem.

- The FSB was tasked by the G20 to better understand cyber risks, including a stock-take of existing cyber security regulation, as a basis for developing best practices, and found considerable differences across jurisdictions.

Important Focus Areas

- Enhanced collaboration between private and public sector.
- More effective information sharing initiatives, including cross-border.
- Efforts to create a common language and taxonomy for reporting purposes.
- More coordinated approaches to the proliferation of penetration testing exercises.
- Promoting the role of the home supervisor as a “one stop shop” mechanism to provide host and other supervisors with information on the cyber resilience of a particular firm.
- The importance of cross-sectoral approaches, which also address vulnerabilities emanating from outside the financial system.
- Encouraging rating systems that provide comparable assessments of an individual institution’s cyber resilience.

IIF–GFMA Operational Resilience Principles

Draft Principles Supporting the Strengthening of Operational Resilience Maturity in Financial Services (Oct 2019)

1. The global financial industry should embrace the importance of operational resilience.

2. Operational resilience is a global effort that will require the adoption of an international common approach by the public and private sectors.

3. Industry will seek to work with regulators to establish a global common lexicon and taxonomy to promote consistency and alignment across all markets.

4. The approach to operational resilience for the financial industry should be risk-and principles- based, reflecting each participant's respective risk profile, appetite and tolerances.

5. Dependencies and connectivity between the financial sector, the financial sector, utilities, critical infrastructure and critical shared services must be transparent.

Collaboration across sector, with authorities

There are also a number of information-sharing platforms in place that encourage financial institutions, in cooperation with authorities, to share intelligence on attacks:

- Real-time incident reporting, anonymized with patches
- Importance of cross-sectoral approaches

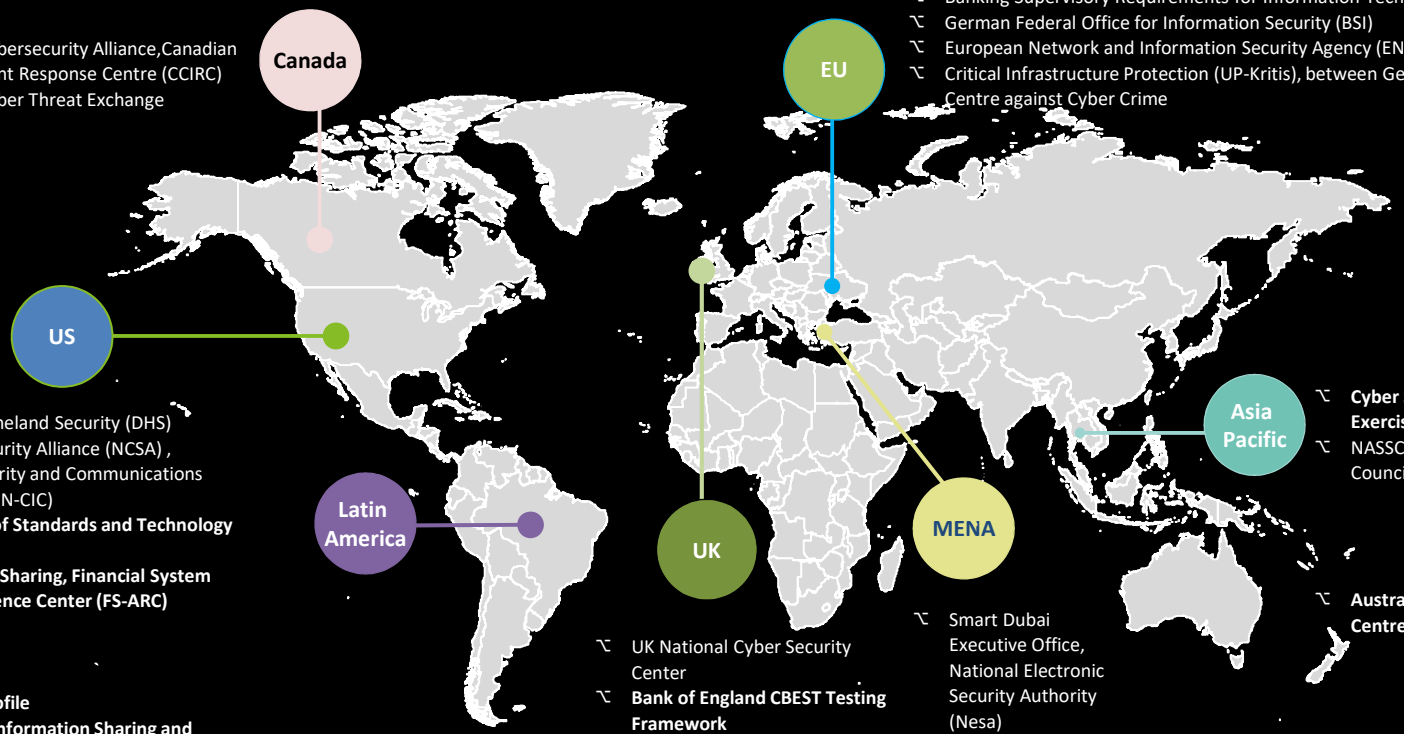
Working together with government and law enforcement:

- Sharing of strategic trends
- Penetration testing exercises (role of Home supervisor)
- Cross-border initiatives

Common standards and approaches

- Regulatory coherence
  - Addressing fragmentation; common terms (lexicon) and approaches
- Information-sharing
  - Real-time and strategic across industry and with authorities
- Pen-testing
  - “Table-tops”, stress tests, simulations
- Industry frameworks
  - Common language and standards, such as U.S. NIST, CPMI-IOSCO
- Certification
  - Possible third party “clean bill of health” post-attack certification

Common standards and approaches



- Canadian Cybersecurity Alliance,Canadian Cyber Incident Response Centre (CCIRC)
- Canadian Cyber Threat Exchange

- **IOSCO**
- Banking Supervisory Requirements for Information Technology (BAIT)
- German Federal Office for Information Security (BSI)
- European Network and Information Security Agency (ENISA)
- Critical Infrastructure Protection (UP-Kritis), between German Competence Centre against Cyber Crime

- Department of Homeland Security (DHS)
- National Cyber Security Alliance (NCSA) , National Cybersecurity and Communications Integration Center (N-CIC)
- **National Institute of Standards and Technology (NIST)**
- **Threat Intelligence Sharing, Financial System Analysis and Resilience Center (FS-ARC)**

- **Cyber Security Agency (CSA) – Exercise Cyber Star**
- NASSCOM – Data Security Council of India (DSCI)

- **Australian Cybersecurity Centre**

- UK National Cyber Security Center
- **Bank of England CBEST Testing Framework**

- Smart Dubai Executive Office, National Electronic Security Authority (Nesa)

GLOBAL:
- **Financial Sector Profile**
- **Financial Services Information Sharing and Analysis Center (FS-ISAC)**
- **FSB Cyber Lexicon**
- **IIF-GFMA Operational Resilience Draft Discussion Principles**

Conclusions

- Current threat landscape
  - Challenging and need for public-private defense
- How the industry is responding
  - Focus on resilience, avoiding market fragmentation
- The emerging regulatory response
  - Developing standards, role of global standard setters, need for a common Lexicon
- Building partnerships around resilience
  - Many areas where PPP are needed and being developed