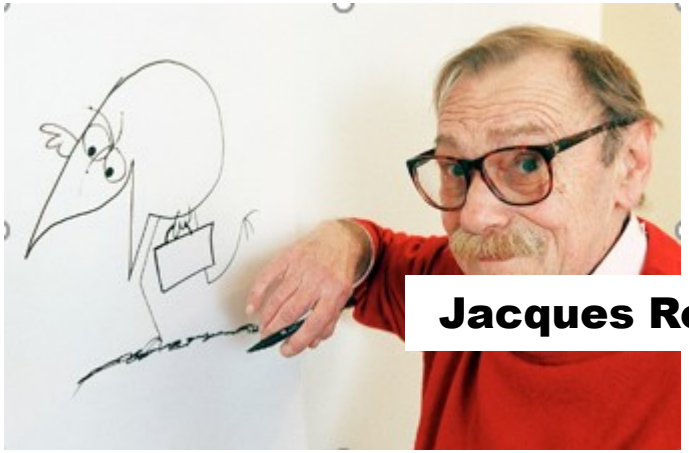
IT & CYBER RISK,

MANAGING IT/CYBER RISK FROM AN OPERATIONAL RISK PERSPECTIVE

Gilles Mawas (BNP Paribas)
Paris, 5 July 2019

« Le passé ne sera jamais pire que l'avenir »

« Il vaut mieux pomper même s'il ne se passe rien, que de risquer qu'il se passe quelque chose de pire en ne pompant pas »



0 Operational risk

I A business risk

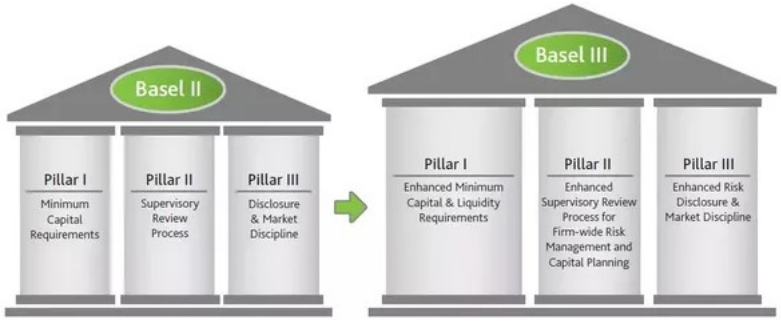
II An emerging risk

III How to manage this business risk

IV Conclusion

Credit, market, liquidity… risk and operational risk

Operational risk



The *financial* risk

- Credit, market, liquidity…

The *operational* risk

- All non financial risks as defined per Basel II/III, including
  - Fraud
  - IT / cyber
  - Compliance
  - Process, product...

The *reputation/image* risk

- Not explicitly taken into account

BANK FOR INTERNATIONAL SETTLEMENTS

What is an operational risk

- Definition of operational risks

  Operational risk is defined as the risk resulting from the inadequacy or **failure** of **internal processes**, or from **external events**, that has resulted, could result or could have resulted in a **loss**, a **gain** or lost earnings (fraud, natural catastrophe, human error, IT failure…).

- Operational risk management – three goals

  1. avoid ***losses***
     - to avoid a financial industry ***systemic failure***
     - protect the ***bank P&L***
  2. optimise ***regulatory capital*** / RWA
  3. optimise ***costs*** – under- protection / over-protection

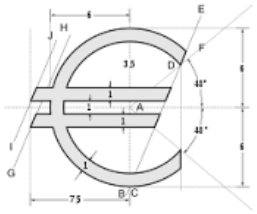
The way you do not want to talk to business…

A business perception mostly based on the impact

The business perceives IT risk mostly through its direct impacts: theft, data leakage and service disruption

Theft

- direct loss of **clients** assets (cash, securities…)
- direct loss of the **bank** own assets (cash, securities…)
- loss of valuable information (commercial files, business models [algos…]…)
  - probable cause: human error, internal/external actor, malware...
  - consequence: direct loss, regulator fine…



Data leakage (client and bank data)

- accidental loss of data
- voluntary theft of data
  - probable cause: human error, internal/external actor, malware...
  - consequence: regulator fine, loss of business

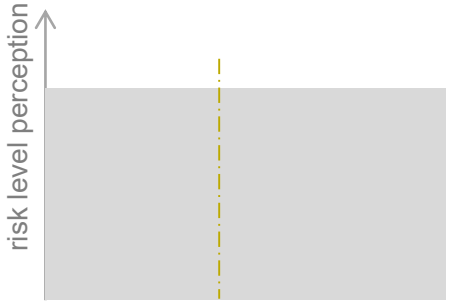
Service disruption

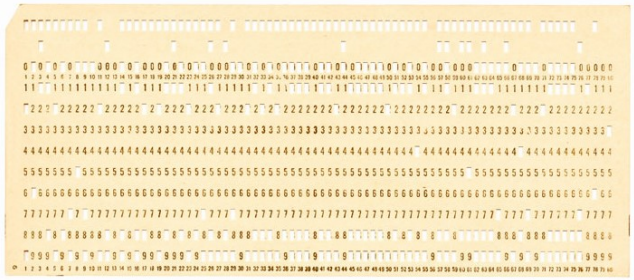
- application unavailability
- inability to access to applications (client, user…)
  - probable cause: software bug, hardware failure, external event (flood…), cyberattack (DDoS), sabotage (internal), network issue…
  - consequence: inability to generate revenues, fine from regulator, client penalty…

IT risk, cyber risk, evolving perception… (classic IT risk)

The ‘classic’ IT risk

- as managed since IT inception (60’s) – **hardware failure**, software **bugs**, unauthorised accesses…
- historical incidents collection (both the bank and the whole financial industry) – being recorded since start of operational risk inception, no major increase

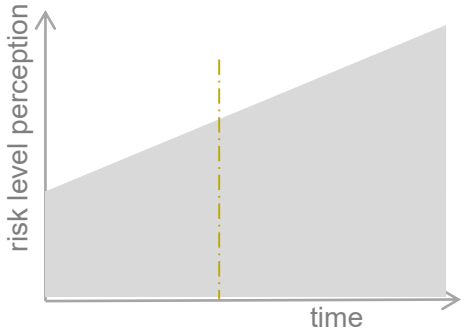




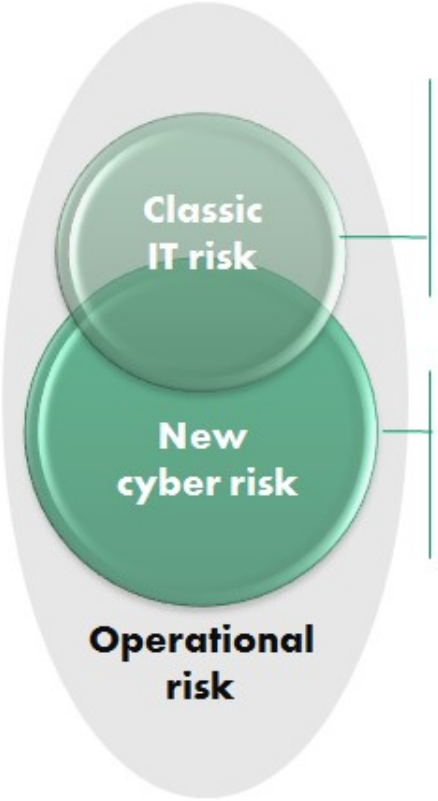
IT risk, cyber risk, evolving perception… (new cyber risk)

The 'new' cyber / IT risk

- born with internet, ever growing and evolving (virus, malware, ransomware…)
- historical incidents collection (both the bank and the whole financial industry) – very low number recorded but exponential increasing as reported by press and consulting firms

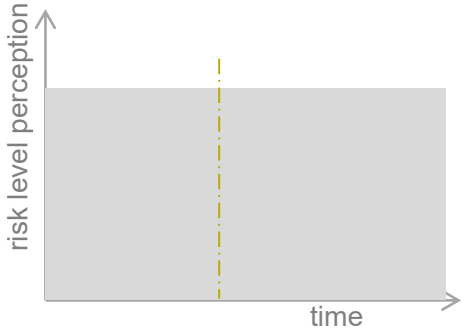


IT risk, cyber risk, evolving perception…



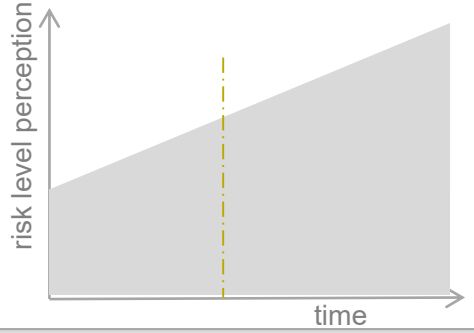
The 'classic' IT risk

- as managed since IT inception (60's) – hardware failure, software bugs, unauthorised accesses…
- historical incidents collection (both the bank and the whole financial industry) – being recorded since start of operational risk inception, no major increase



The 'new' cyber /IT risk

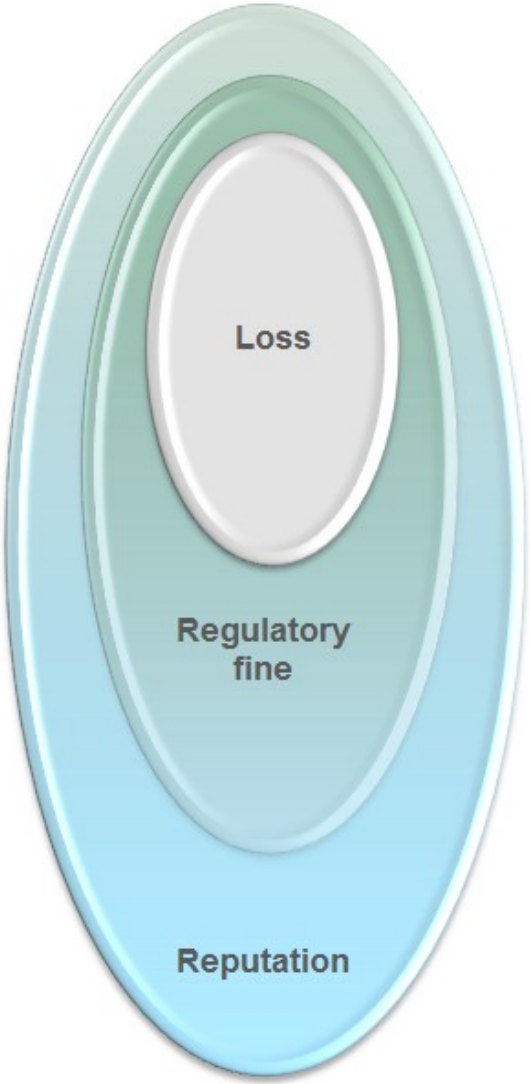
- born with internet, ever growing and evolving (virus, malware, ransomware…)
- historical incidents collection (both the bank and the whole financial industry) – very low number recorded but exponential increasing as reported by press and consulting firms



Overall, the cyber / IT risk is **perceived as very high**, and **increasing**…

- by our **clients**
- by our **regulators**
- By our own **personnel**
- by our **general management**
- and by the **general public** (press, social media…)

Three dimensions with potentially dramatic impacts…



Assets Loss, thef

Information Theft

Continuity of service Outage, s

Cyber regulations,

Data protection,

Banking secrecy regulations and la

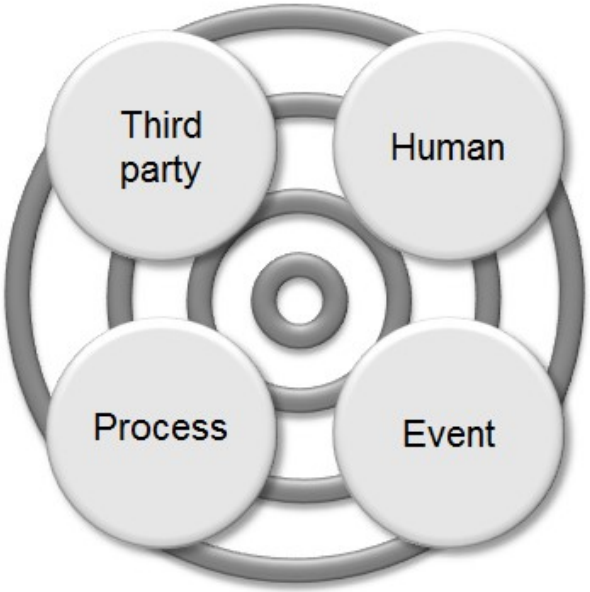
Reputation & image impact (*not a measurab Basel*): Market capitalisation, opportunity cos trust, brand value…

Understanding the origins of incidents…

Third party

Accidental – event or error
Malevolent – attack on bank assets

Human
(both staff and non staff)
Accidental – Human error
Malevolent – Activist, competitor, employee



Process flaw
Quality – Poor design / lack of test
Accidental – Design loophole
Malevolent – Back door

External event

Accidental – natural hazard, outage
Malevolent – Malware injection, DDOS

… but never forget about the human dimension

"Companies spend millions of dollars on firewalls, encryption and secure access devices, and it' is wasted money, because none of these measures address the weakest link in the security chain."

Kevin Mitnick – ethical hacker

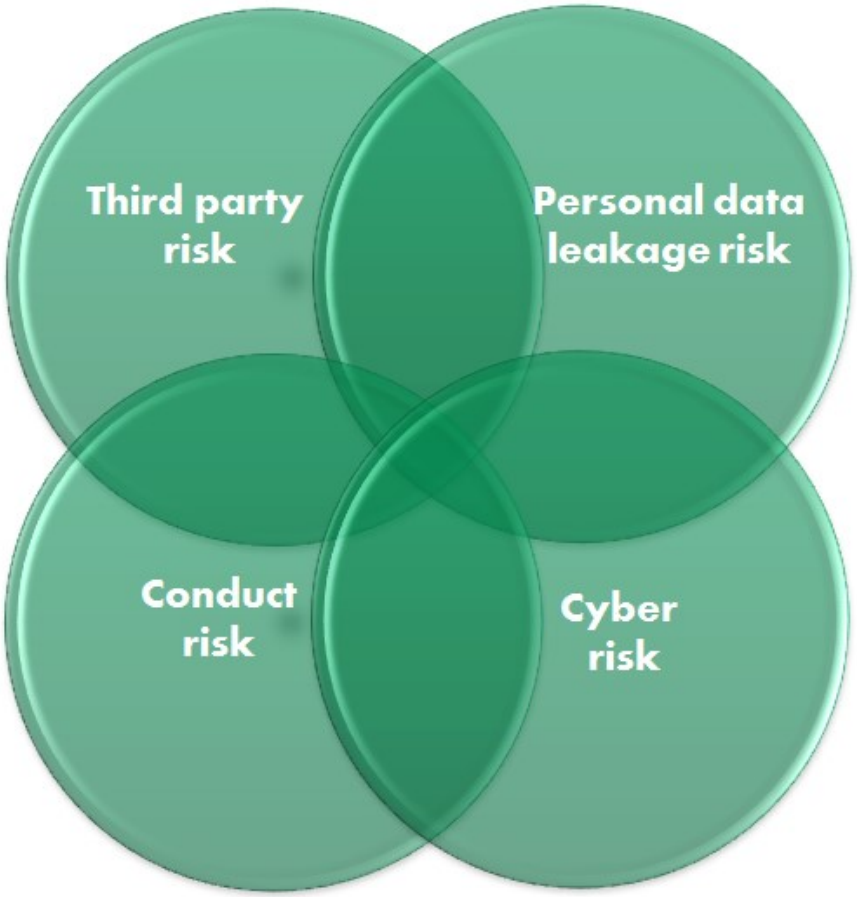
I A business risk

II An emerging risk

III How to manage this business risk

IV Conclusion

Four new “emerging & transversal” risks …



These four transversal risks

- are perceived as **growing** and **large investments** are dedicated to them
- may result in incidents in **several Basel II event** type category (1 to 7)
- are subject to **specific regulations**, on top of the regular Basel II one
- are not always **clearly defined** and **overlap** with other categories
- do **not** have a **long history** of past events (in incident databases)
- and they are **overlapping**…

….with very large investments/spending…

CYBERSECURITY VENTURES

Cybersecurity Ventures predicts global spending on cybersecurity products and services will exceed $1 trillion cumulatively over the next five years, from 2017 to 2021.

In 2004, the global cybersecurity market was worth $3.5 billion — and in 2017 we expect it to be worth more than $120 billion. The cybersecurity market grew by roughly 35X over 13 years.

Forbes January 2016

Why J.P. Morgan Chase & Co. Is Spending A Half Billion Dollars On Cybersecurity

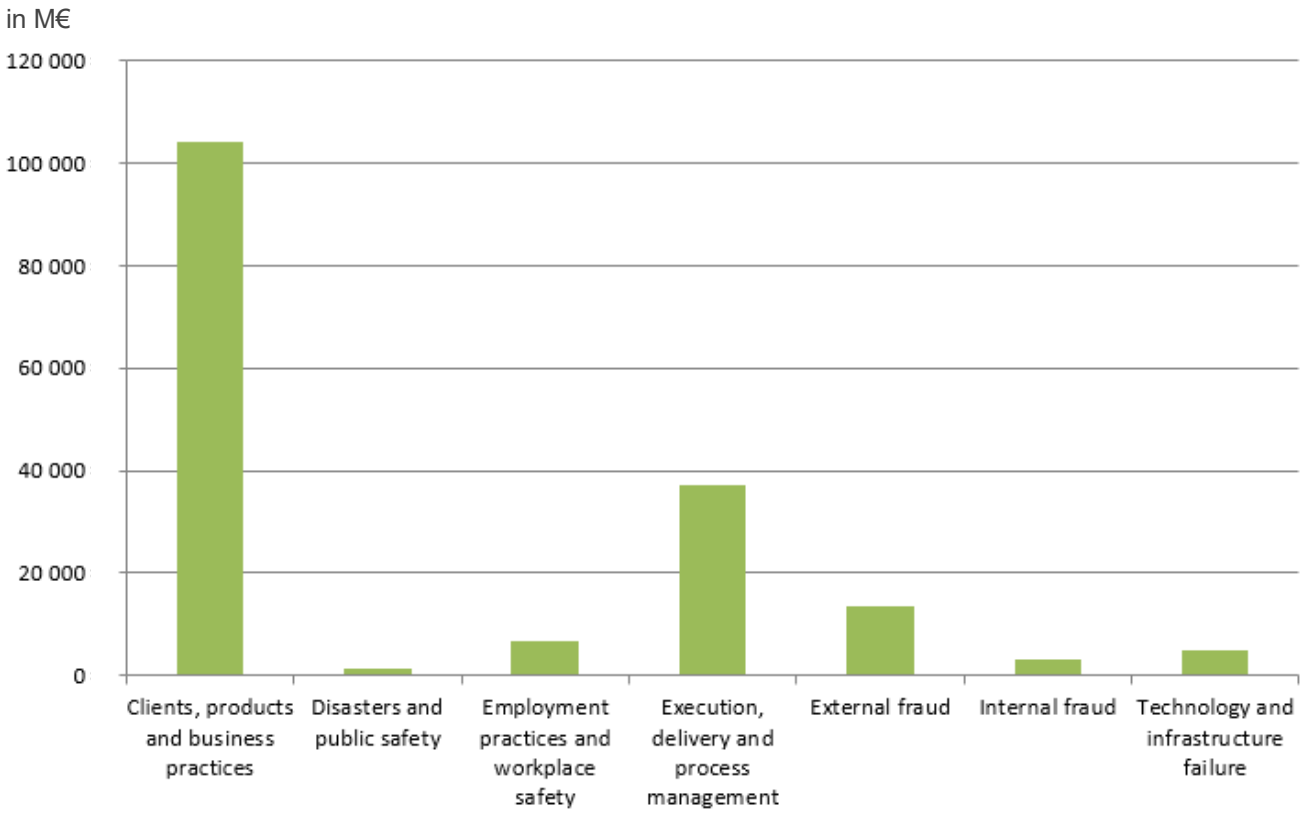
SecurityScorecard R&D Department
August 2016

HOMELAND SECURITY RESEARCH

According to Homeland Security Research's U.S Financial Services: Cybersecurity Systems & Services Market report, the U.S. financial institution's cybersecurity market is the largest and fastest growing in the private sector, predicted to grow to $68 billion by 2020. Major financial institutions JPMorgan Chase & Co., Bank of America, Citigroup and Wells Fargo spend a collective $1.5 billion on cybersecurity annually.

….but – up to now – relatively modest losses…

ORX – cumulated losses 2012-2017 par event type



#1 type is “Clients, Products and Business Practices” accounting for 67% of
losses and totalling 104b n€ for the years of 2012-2017 losses These incidents are due to unintentional or negligent failure to meet a professional
obligation to specific clients

#2 type is “Execution, Delivery and Process Management” – 22% of loss events (37 b€).
This event type covers losses resulting from failed transaction processing or process management and relations with
trade counterparties and vendors.

Cyber incidents are split among
- Fraud (mainly external)
- Technology failures

These events represent less than 13% on a grand total 171 b€

ORX – cumulated losses 2012-2017 par event type/business

Figure 1. The number of events submitted in each business line and event type between 2012 and 2017

IT/cyber threats – but no large historical losses…

Historical figures – from ORX

ORX (100+ affiliates) – private sources (members only – anonymised)

- Financial services (banking, insurance and asset management) – from 2009 to 2017
- All Basel event types – threshold > 20 k€
- Number of cyber related incidents / all incidents over **8** years
  - **2,300** / 525,000 less than **0,5%** in number of incidents
- Amount of cyber related incidents / all incidents
  - **208 M€** / 350,000 M€ less than **0,06%** in loss amount

ORX News – public sources (news, conference, web…)

- Financial services (banking, insurance and asset management) – from 2002 to 2017
- All Basel event types – threshold >1 M€
- Number of reported cyber related incidents over **15** years
  - **315** incidents reported – including 223 without published loss amount
- Amount of cyber related incidents over **15** years
  - Total losses = **4 b€** including large Brazil cyber (2012-2014) incident **2,8 b€**

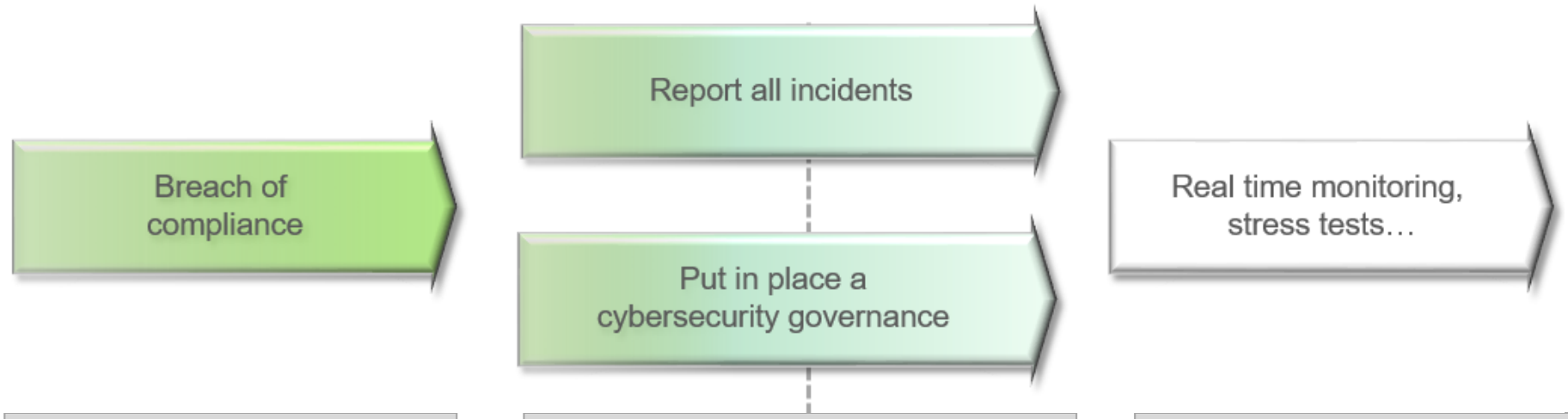
I A business risk

II An emerging risk

III How to manage this business risk

IV Conclusion

The regulatory framework is evolving too at fast pace



Application of current regulations/ laws

Business - financial security
Data - banking secrecy
Data - personal data
Finance/Risk regulatory reporting
- timely and accurate

Consumer/client protection
- safeguard assets + quality of service

Regulations/ laws being deployed

USA - NY-DFS (governance) – start 2017
HK – HKMA (report incidents), SFC (governance and report)… - active
SN – MAS (incident), new cybersecurity bill (expected in 2017 on governance)
EU - GDPR (personal data), Network & Information Security Directive – active in 2018
UK – FCA - active
LX – CSSF circulars (incident) - active

Emerging regulations/ laws

Basel III/IV
EU, USA, UK…

I A business risk

II An emerging risk

III How to manage this business risk

IV Conclusion

Conclusion

As other major financial risks, IT/cyber risk needs to be managed as a **strategic business** risk,

- involving **all stakeholders** (business, IT, Risk, CISO…) with a clear (but adaptive) **governance**
- moving from an IT managed topic to a bank-wide concern, requiring an 'almost real time' **monitoring**
- according to a clearly stated **risk appetite**, periodically reviewed

We need a **mature** but **adaptive** IT/cyber risk management **framework**

Merci