

Cyber Insurance Trends

Verengai Mabika
Senior Policy Advisor - Africa



Cyber Insurance – market dynamics

The cost and risks of cyber attacks are increasing

Cyber Threat Landscape

- Cybersecurity events and costs are increasing:
 - 79% of survey respondents detected a security incident in the past 12 months¹
 - Average total cost of a data breach increased 23% over the past two years²
 - Average cost paid for each lost / stolen record increased 6%¹

Industry Outlook

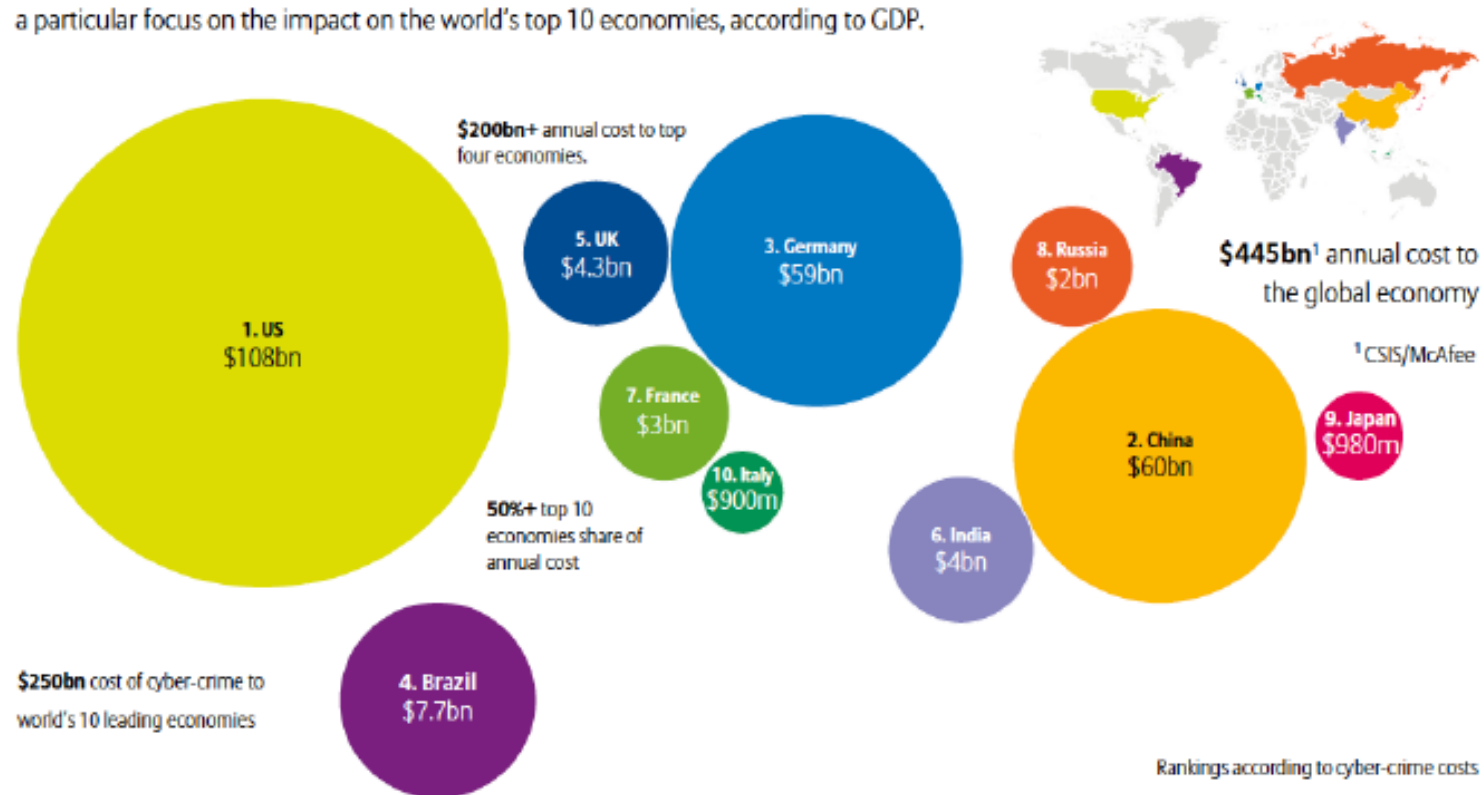
- Data breaches are expected to reach \$2.1 trillion globally by 2019³
- 76% of survey respondents¹ were more concerned about cybersecurity threats than in previous 12 months:
 - Increase from 59% in 2014

Reputational Risk

- An IT security breach can have serious implications in how a company is perceived:
 - 46% of companies suffered damage to reputation & brand value due to a security breach⁴
 - 19% of companies suffered damage to reputation & brand value due to a third-party security breach or IT system failure⁴
- The risk of losing customer trust is significant and rising:
 - 82% of customers would consider leaving an institution that suffered a data breach⁵












How much does **cyber-crime** cost the world's leading 10 economies?

This **AGCS** atlas examines the estimated total cost to the global economy from cyber-crime per year, with a particular focus on the impact on the world's top 10 economies, according to GDP.



Country Ranking by GDP ¹	Cyber-crime as a % of GDP ²	Estimated cost ³	Country Ranking by GDP ¹	Cyber-crime as a % of GDP ²	Estimated cost ³		
1 US	\$16.8trn	.64%	\$108bn	6 UK	\$2.7trn	.16%	\$4.3bn
2 China	\$9.5trn	.63%	\$60bn	7 Brazil	\$2.4trn	.32%	\$7.7bn
3 Japan	\$4.9trn	.02%	\$980m	8 Russia	\$2.1trn	.10%	\$2bn
4 Germany	\$3.7trn	1.60%	\$59bn	9 Italy	\$2.1trn	.04%	\$900m
5 France	\$2.8trn	.11%	\$3bn	10 India	\$1.9trn	.21%	\$4bn

Breakdown of key statistics for In-Scope countries:

	 Population (2016 Est.)	 GDP (2016)	 Internet users & subscribers (2016)	 Estimated Cost of cyber-crime (2016)	 Estimated No. of Certified Professionals
 Africa	1,185,529,578	\$2.89T	340,783,342	\$2B	6892
 Nigeria	186,879,760	\$481.066B	97,210,000	\$550M	1500
 Kenya	46,790,758	\$63.398B	37,716,579	\$175M	1400
 Tanzania	52,482,726	\$44.895B	17,263,523	\$85M	250
 Ghana	26,908,262	\$37.86 B	19,125,469	\$50M	460
 Uganda	38,319,241	\$26.369B	14,564,660	\$35M	300

*Certified Professionals is limited to the following certifications: CISA, CISM, GIAC, SANS, CISSP, CEH, ISO 27001 and PCI DSS QA

*Economic and internet usage data extracted from respective country Internet regulator reports and World Bank site.

Malawi Veep to lead in cyber security meeting

SECURITY

| April 24, 2015, 6:39 a.m.



Tanzania creates first cyber-crime laws

September 11, 2013 • East Africa, Online

Like 8 Tweet 43 Share 19 +1 Pin it

Cyber crime worries Zambian police

Published on 06 October 2014
By Michael Malakata

Mobile Money Revolution Rises Cyber Security Risk In Africa

By Kevin Mwanza **AFKI Original**
Published: June 12, 2014, 9:08 am



US Man Sues Ethiopian Government for Spyware Infection

By AFP on February 19, 2014

Rwanda National police warns internet users against cyber crime

The Observer (Kampala) »

19 AUGUST 2015

Uganda: Banks, Telecoms Remain Top Cybercrime Targets - Experts

Tagged: Business • East Africa • ICT • Legal Affairs • Uganda

How developed is Cyber Security in select member countries?

- Report developed by International Telecommunication Union (ITU)
- Key indicators for cyber security development are:
 - Legal
 - Technical capacity
 - Organizational
 - Capacity Building
 - Cooperation



Country	GSI Rank
Mauritius	1
Uganda	2
Rwanda	3
Kenya	5
South Africa	6
Tanzania	11
Botswana	12
Malawi	12
Zambia	13
Burundi	14
Angola	15
Mozambique	16
Swaziland	16
Zimbabwe	17
Ethiopia	17
Namibia	18
Lesotho	18

Source: GLOBAL Cybersecurity Index & Cyberwellness Profiles Report 2015

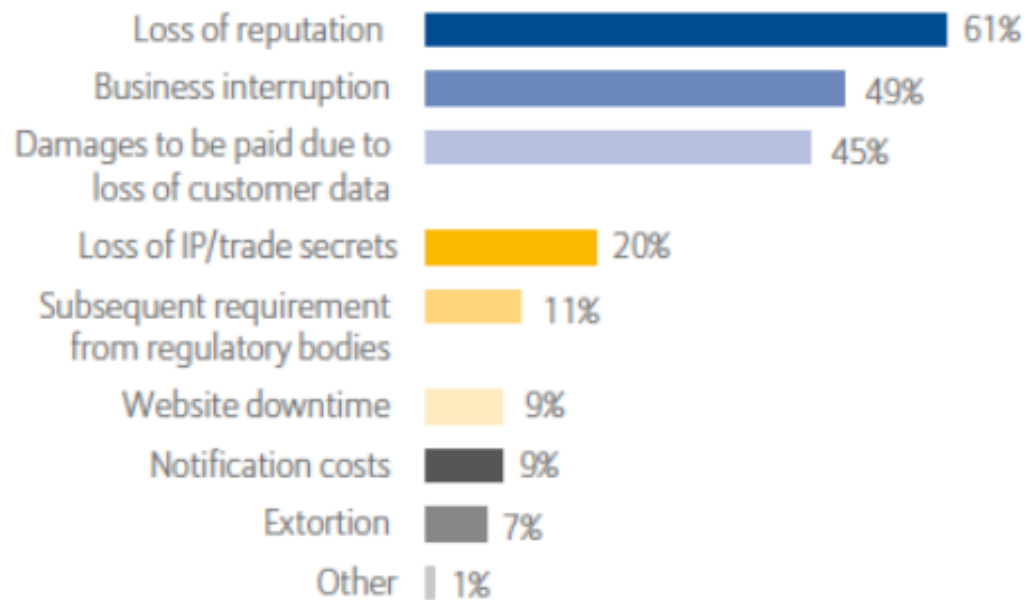
Cyber Risk

- any risk of **financial loss, disruption** or **damage to the reputation** of an organisation from some sort of **failure of its information technology systems** (*includes networks & the internet*).

Where is the market headed?

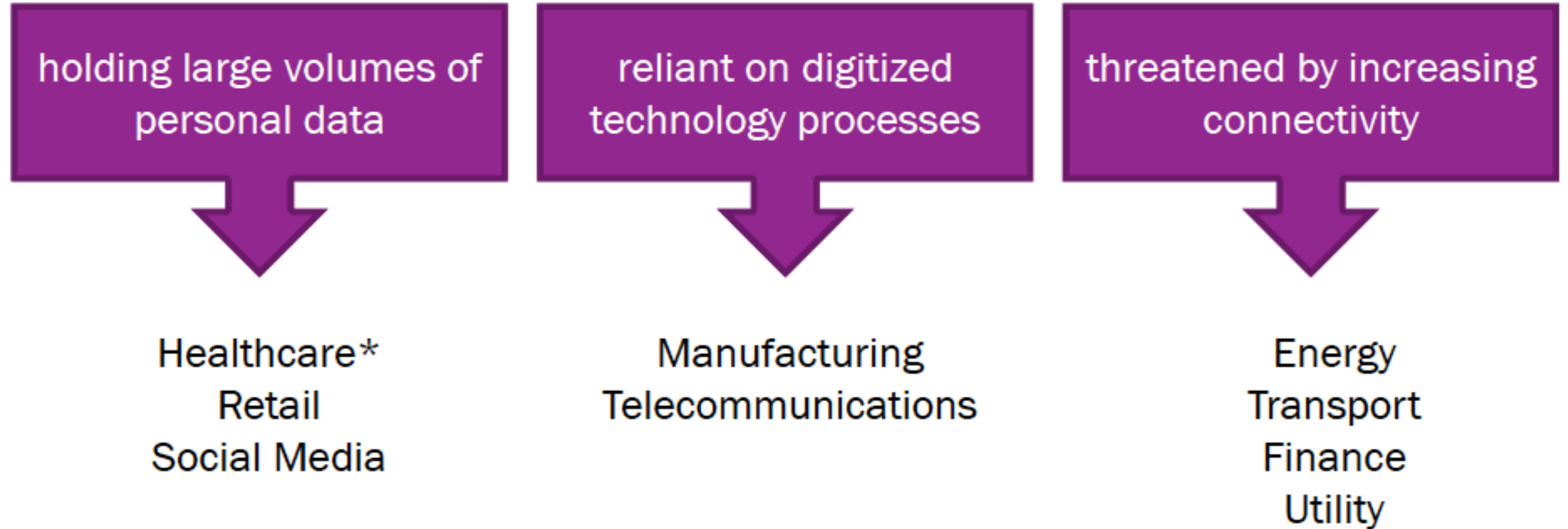
“The pace of change is slow in insurance. [Real change] will be slower than [in] other industries. The question is when it will happen – 5, 10, 20 years?” -Anonymous Director

Which cyber risks are the main cause of economic loss?



- Few new products or services being offered by insurers
- Move from selling products to comprehensive services

Sector Trends: Current and Future Insurance Customers



Cyber Insurance Coverages fall into 4 categories:

- 1. Liability**—defense and settlement costs for the liability of the insured arising out of its failure to properly care for private data
- 2. Remediation**—response costs following a data breach, including investigation, public relations, customer notification, and credit monitoring
- 3. Regulatory Fines and/or Penalties**—the costs to investigate, defend, and settle fines and penalties that may be assessed by a regulator; most insurers do not provide this coverage, although there can be coverage for defense costs
- 4. PCI (Credit Card) Fines and Penalties**, including forensic services and card reissuance costs

Regional Trends

North America: 87% of the overall cyber insurance market

Mandatory legislation in several U.S. states

2015: U.S. insurance industry generated \$1 billion in direct written premium volume for cyber insurance

Europe: Incoming 2018 regulations regarding data protection and security

Asia Pacific: Negligible

Projected to increase due to ransomware

Conclusion

- Cyber risk is an emerging risk in the world
- Legal framework for insurable legal liability is generally under development across east & southern African countries
- There is demand for cyber risk insurance
- Where pricing data is not available – proxies can be developed
- Underwriting will depend on risk management and culture of the client