

# Cyber Security Strategy

## Khartoum



Ali Mukrid  
Group CISO

**Ecobank**  
The Pan African Bank

# Contents

The background of the slide is a light blue, semi-transparent image. It features a computer keyboard in the lower-left corner, a mouse in the lower-right corner, and a stylized binary code (0s and 1s) running diagonally across the right side. There are also some abstract, glowing lines and shapes that suggest a digital or network environment.

- Definition, Drivers & Approach for Cyber Security
- Threat Background
- Global Threat Outlook
- Africa Threat Outlook

# Definition

---

Information Security is the protection of organization's information assets from unauthorized access, use, misuse, disclosure, destruction, modification or disruption.

This involves maintaining the :-

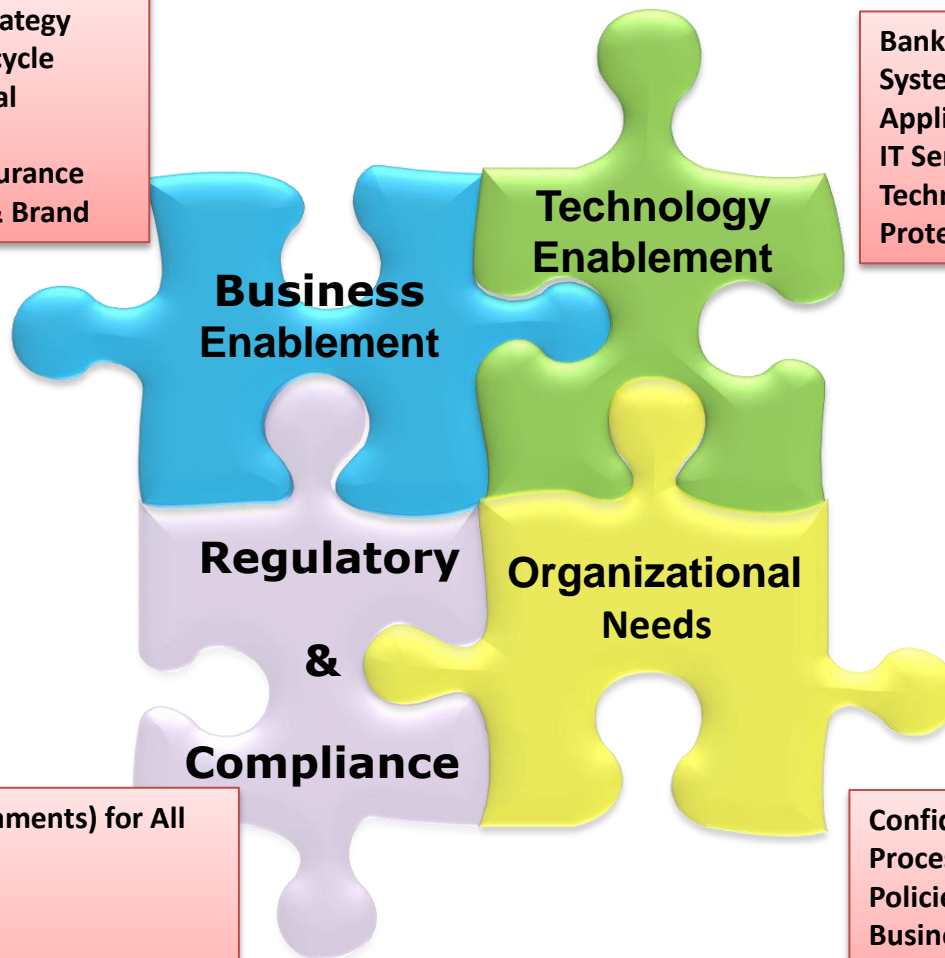
- Confidentiality of information
- Integrity of information
- Availability of information

This further includes protecting systems that house, process and transmit information. Today information assets are found in every aspect of any business or service.

The process and capability of such information protection involves Skilled Resources, Technologies and Processes & Procedures embedded as part of Business as Usual Operations.

Financial Institutions through offering banking services to customers, store, process, and transmit wide range of informational assets of varying degree of sensitivity including and not limited to customer personal data, transaction data, accounting data etc.. To achieve defined business objectives.

# Drivers for Security Strategy, Business Enablement, Governance, & Compliance



Business Requirements/strategy  
Product Development Lifecycle  
Digital Services/Commercial  
roadmap  
Shareholder /Business Assurance  
Protection of Investment & Brand

Banking Infrastructure  
Systems Infrastructure  
Applications Infrastructure  
IT Services  
Technology Security Assurance  
Protect & Defend Technology Assets

Regulatory  
&  
Compliance

Organizational  
Needs

Regulatory Authority ( Governments) for All  
affiliates  
Industry regulation  
Cyber Laws Compliance  
Corporate Emergency Crisis Management  
National Emergency Crisis Management

Confidentiality, Integrity & Availability  
Process Controls  
Policies Procedures & Standards  
Business Continuity, DR, BCP  
Information Assurance

# Information Security Objectives and Priorities

## Objectives:-

Protecting the Bank from computer related crime emanating from either internal or external.

## Priorities:-

- Protecting the Perimeter dividing internal and external network
- Protecting key infrastructure through implementing appropriate information security related controls
- Elevating the level of staff and customer information security awareness to mitigate current threat level
- Embed and Operationalize information security in line with business strategy and objectives

# Global Risks and Threats Outlook



*Present and Future Threat Outlook*



# Review Globally

Cyber-Safe

## Bangladesh central bank chief resigns after \$101 million heist

by Charles Riley and Sugam Pokharel @CNNTech

🕒 March 15, 2016: 7:35 AM ET

👍 Recommend 1K 📧 📱 📺 📷 📧 ⋮




**HACKERS STEAL UP TO \$1 BILLION FROM BANKS** **CNN** 7:21 AMPT

LITTLE ROCK, AR	CURRENT CONDITIONS	TEMP	WIND CHILL	DIRECTION	WIND
Overcast Freezing Rain		28°	20°		

00:08 / 02:31

Hackers steal up to \$1B from more than 100 banks

### Social Surge - What's Trending



Match.com pulls ads after freckle furor



Volvo promises deathproof cars by 2020



Mark Zuckerberg talks drones, bots -- and takes a jab at Trump

IN ASSOCIATION WITH  
**AUDEMARS PIGUET**  
*Le Brassus*



glo

\*1057#

The chief of Bangladesh's central bank has resigned after losing \$101 million in a bank heist that spanned at least four countries

# Review Globally



## 1) Target

- Major US Retailer
- 40 Million Credit and Debit card Records
- 70 Million Data files of customers

NEW YORK (AP) — Target's CEO has become the first boss of a major corporation to lose his job over a breach of customer data, showing how responsibility for computer security now reaches right to the top.



110  
MILLION  
IMPACTED  
CUSTOMERS





# Review Globally



## 1) Home Depot

- Home Improvements retailer
- 53 Million customer records stolen including credit cards



1. [Hack attacks hit home: 'The kind of thing that CEOs get fired for'](#)

2. Financial Post-02 Feb 2015

3. Fotolia Hack attacks have forced the resignations of CEOs at ... at Target Corp., Home Depot, Sony Pictures Entertainment, and Wall Street giant ...

4. [Critical Infrastructure Vulnerable to Cyber Attacks](#)

NBC Bay Area-01 Feb 2015 [Explore in depth](#) (6 more articles)



1. [Home Depot confirms months-long hack](#)

2. CNNMoney-08 Sep 2014

3. Home Depot on Monday confirmed that hackers indeed broke into its payment systems -- maybe as far back as April. Home Depot (HD)'s hack ...

4. [Home Depot Confirms](#)

Business Insider-08 Sep



# Growing Risks and Threats Outlook of 2015 >

## Top 10 Global Business Risks for 2015



To see full Risk Barometer 2015 rankings click here

Source: Allianz Global Corporate & Specialty, For methodology, see page 7

Allianz Risk Pulse

## Allianz Risk Barometer Top Business Risks 2015

### Risk and reputation in the age of disruption

Business interruption (BI), cyber, political upheaval, tech innovation and climate change top risks for 2015 and beyond

- Traditional industrial concerns including natural catastrophes and fire head annual Allianz Risk Barometer.
- Businesses face new challenges posed by today's interconnected corporate environment.
- Increasing number of non-property damage risks – including cyber and geo-political disruption – can impact a company's balance sheet and reputation.

"Risk management must reflect this reality. The root cause of many losses can often be traced back to the planning phase. Identifying the impact of any interconnectivity early can mitigate or help prevent losses occurring. Fostering cross-functional collaboration within companies is essential to tackle modern interconnected risks."

Business interruption (BI) and supply chain, natural catastrophes and fire/explosion are the major risks which occupy the attention of companies at the start of 2015, according to the fourth annual Allianz Risk Barometer, which surveys over 500 risk managers and corporate insurance experts from more than 40 countries.

Cyber risks is the most significant mover in this year's Risk Barometer and is also the top emerging risk for the next five years. Yet although awareness increases, it is still the top risk underestimated by business, with budget constraints cited as one of the main reasons why companies are not more prepared for the disruption caused. According to the Risk Barometer, loss of reputation or brand value is now the main cause of economic loss for businesses in the event of a cyber incident, even higher than costs resulting from the interruption.

However, businesses are also increasingly concerned about a number of emerging perils from today's complex global business environment. "The growing interdependency of many industries and processes means businesses are now exposed to an increasing number of disruptive scenarios," says Chris Fletcher Hirs, CEO, AGCS.

Allianz



# Growing Risks and Threats Outlook of 2016

## Top 10 Global Business Risks for 2016



To see full Risk Barometer 2016 Rankings click here

For methodology, see page 3. Source: Allianz Q&A Corporate & Specialty

Allianz Risk Pulse

## Allianz Risk Barometer Top Business Risks 2016

### Executive Summary

The fifth annual Allianz Risk Barometer identifies the top corporate perils for 2016 and beyond, based on the responses of more than 800 risk experts from 40+ countries around the globe.

Business interruption (incl. supply chain disruption), market developments (volatility, intensified competition and market stagnation) and cyber incidents are the top three global business risks. Business interruption (BI) is top for the fourth year in succession.

▶ page 3

The risk landscape is changing. Businesses face a wider range of disruptive forces in 2016 and beyond. The effects of globalization, digitalization and technological disruption pose fundamental challenges to many business models.

▶ page 4

Businesses and insurers must review their insurance and risk mitigation needs to reflect this new risk management reality. Reining existing, and developing new, risk services will be necessary.

▶ page 4

Interconnectivity of risk continues to grow. Many of the top 10 risks such as natural catastrophes, fire, explosion, cyber incidents and political risks can have severe BI implications. Businesses are increasingly concerned about their impact; political instability can have on supply chains.

▶ page 5

Market developments is the second top risk. Many industrial sectors are facing tougher operating conditions, including intensified competition from new areas.

▶ page 7

Businesses are more concerned about cyber incidents, which is the top long-term risk and the peril most likely to increase the threat of BI. Hackers are not the only problem. Operational technology issues also result in major system interruptions.

▶ page 10

Digital and technological innovations and transformations, such as Industry 4.0, bring new risks in addition to benefits. Increasing sophistication of cyber-attacks is the impact of increasing digitalization; businesses fear most. Many companies have insufficient knowledge and budget to mitigate the risk, as the threat continues to evolve.

▶ page 12

There are significant differences in the top 10 risks around the world. Macroeconomic developments tops the Africa & Middle East rankings. Cyber incidents is the number one risk in the UK.

▶ page 14

Allianz

# Top Risks in Focus :- Cyber incidents



In today's interconnected world of internet-based supply chain management, a simple technical failure can result in a major system interruption.

Photo: Shutterstock

## Top risks in focus: Cyber incidents



Cyber risk connected: 12 ways in which a business can be exposed

Cyber risk appears in many forms, all of which can represent major threats to business. Companies increasingly face new exposures, including first- and third-party damage, business interruption and regulatory consequences.

**\$445bn a year**

It is estimated that cyber-crime alone costs the global economy approximately \$445bn a year, world's largest economies accounting for 70% of this, data analyzed in an AGCS report. *Cyber Risk: Managing The Impact of IT Interconnectivity* shows. The threat of cyber incidents is expected to increase further.

According to Symantec Corporation<sup>2</sup> risks associated with the increasing use of Apple devices and "Internet of Things" are among the factors that drive this increase. The US software security firm predicts that attacks on critical infrastructure will also rise.

"Internet of Things" Describes a future where all the devices we use are connected to the internet, allowing them to send and receive data.

This increasing risk is reflected in the Risk Barometer with cyber incidents (cyber-crime, data breaches, IT failures) gaining 11 percentage points year-on-year to move into the top three risks for the first time (28%). Three years ago this peril ranked just 15th (6%).

Loss of reputation (69%) is the main cause of economic loss for businesses after a cyber incident, according to responses, followed by business interruption (60%) and liability claims after a data breach (52%).

Due to the almost automatic blow a company's reputation can sustain in the event of a cyber incident many attacks still go unreported. However, many network outages and disruptions, that are not caused by cyber-attacks, but by technical issues, are not made public for similar reasons.

A lack of understanding (48%) of the complexity of the risks involved is cited as the main factor preventing companies from being better prepared to combat cyber threats. Not having a concrete assessment of the cost of the risks involved (46%) ranks second. Budgetary constraints (39%) ranks third.

Cyber Security, at AGCS Financial Lines Central & Eastern Europe.

"Studies show that it takes, on average, 90 days for businesses to discover they have been hacked. Often the incident is identified, not by the business itself, but by the customer or another stakeholder, which is another reason why cyber risks pose a huge threat to a company's reputation.

"The fact that companies often only recognize the loss when an attack has already happened means all they can do is try and prevent further damage. This is why prevention is such a key element in IT security. Managing cyber risk has to be an integral part of any company's risk management strategy."

<sup>1</sup> Net Losses: Estimating the Global Cost of Cyber-Crime, CSIS/McAfee

<sup>2</sup> [www.symantec.com/connect/blogs/symantec-predictions-2016-looking-ahead](http://www.symantec.com/connect/blogs/symantec-predictions-2016-looking-ahead)

# Africa Threat Outlook



*Africa Current and Future Threat Outlook*



# Africa Threat Outlook

---

- Maturity of Control/investments
- Automation/Digitalization – Manual processes dependent
- Internet Penetration rising fast
- Mobile adoption at increasing rate
- Low Cyber Security awareness amongst the population
- Organized Crime including internal collusion
- Challenge to Prosecute offenders

# Threat Example - Ransomware



## Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.



**WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.**

View

95 : 58 : 17

Next >>



**Thank You**