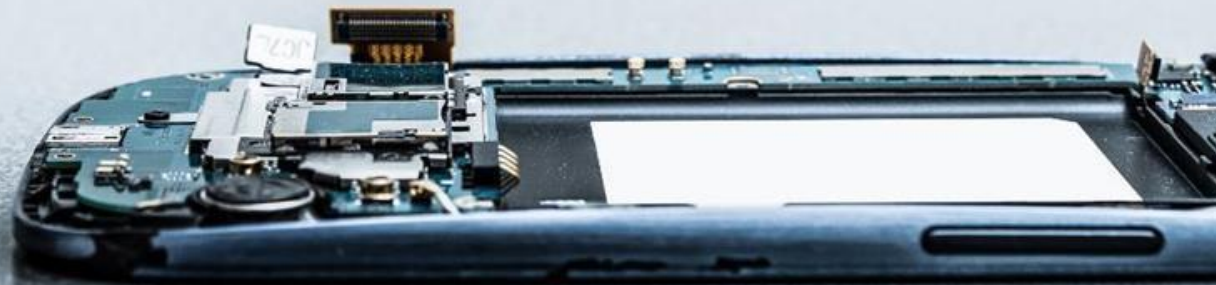


# Workshop on Cyber-Security and Cyber-Risk Insurance Fundamentals



Presentation by **Syed Abdul Qadir**  
16th July 2019



# Speaker's Introduction



## **SYED ABDUL QADIR – Director (Technology Consulting & Risk Assurance)**

*A. F. Ferguson & Co. | a member firm of PwC network*

*BE, MBA, PMP, CISA, ISO 27001 (Lead Auditor), MCITP, HPCP*

- ✓ **17+ years IT management and cyber security consultancy experience with multinational and local private and public sector companies.**
- ✓ **Previously with Pakistan Refinery Limited as Head of Information Technology**

### **Core Area of Expertise :**

- Digital Transformation and Emerging Technologies
- Enterprise Cyber Security Risk Management
- Data Governance, Analytics and GDPR
- IT Audits and risk management
- Technology strategy and governance
- Information Systems Operations & Maintenance
- Business Continuity and Disaster Recovery Plan
- Project Management and Quality assurance
- Cyber security policy procedures and compliance reviews, ISAE 3402
- IT Operations Management (Business Application, Operating System, Database Management System, Network Infrastructure & Services)
- ERP Solution Design Consulting
- Post Implementation Reviews of Business Applications

**Note: Abdul Qadir has led 25+ consultancy and advisory engagements for Banks and FI(s) related to State Bank of Pakistan's "Enterprise Technology Governance and Cyber Risk Management Frameworks". Based on his experience he has also conducted multiple workshops and trainings attended by Senior Professionals from IT, Information Security, Internal Audit, Compliance and Risk Management.**

## *Disclaimer*

*“The views expressed in this presentation are my. own and do not necessarily represent those of any regulator or our employer”*



# *Agenda*

- **Evolving Technology Landscape, Adversaries and Impacts**
- **Global Cyber Security Attacks / Breaches**
- **Most Common Cyber Security Concepts**
- **Synopsis of the SECP directive on Cyber Security Framework**
- **Key Items for Consideration – SECP Circular and Leading Practices**
- **Way Forward / Action Plan**
- **Q & A Session**





“

***Life was so much easier  
when Apple and BlackBerry  
were just fruits.***

”

Anonymous quote on Twitter

APR  
2019

# DIGITAL AROUND THE WORLD IN APRIL 2019

THE ESSENTIAL HEADLINE DATA YOU NEED TO UNDERSTAND GLOBAL MOBILE, INTERNET, AND SOCIAL MEDIA USE



CHANGES IN DATA PROVIDER METHODOLOGIES MEAN THAT DATA ON THIS SLIDE IS NOT DIRECTLY COMPARABLE TO DATA IN OUR PREVIOUS REPORTS

TOTAL  
POPULATION



7.697

BILLION

URBANISATION:

56%

UNIQUE  
MOBILE USERS



5.110

BILLION

PENETRATION:

66%

INTERNET  
USERS



4.437

BILLION

PENETRATION:

58%

ACTIVE SOCIAL  
MEDIA USERS



3.499

BILLION

PENETRATION:

45%

MOBILE SOCIAL  
MEDIA USERS



3.429

BILLION

PENETRATION:

45%



we  
are  
social



we  
are  
social



# A Mobile Networked Planet

5 Billion (2/3) of World's Population is Connected via Mobile

8 Billion Connections Globally → Connected Machines



APR  
2019

# ANNUAL DIGITAL GROWTH

THE YEAR-ON-YEAR CHANGE IN KEY STATISTICAL INDICATORS



CHANGES IN DATA PROVIDER METHODOLOGIES MEAN THAT DATA ON THIS SLIDE IS NOT DIRECTLY COMPARABLE TO DATA IN OUR PREVIOUS REPORTS

TOTAL  
POPULATION



**+1.1%**

APR 2018 – APR 2019

**+82 MILLION**

UNIQUE  
MOBILE USERS



**+2.6%**

APR 2018 – APR 2019

**+130 MILLION**

INTERNET  
USERS



**+8.6%**

APR 2018 – APR 2019

**+350 MILLION**

ACTIVE SOCIAL  
MEDIA USERS



**+6.1%**

APR 2018 – APR 2019

**+202 MILLION**

MOBILE SOCIAL  
MEDIA USERS



**+11%**

APR 2018 – APR 2019

**+342 MILLION**



we  
are  
social



we  
are  
social

JAN  
2017

# DIGITAL IN ASIA-PACIFIC

KEY STATISTICAL INDICATORS FOR THE REGION'S INTERNET, MOBILE, AND SOCIAL MEDIA USERS

TOTAL  
POPULATION



**4.153**  
BILLION

URBANISATION:  
**47%**

INTERNET  
USERS



**1.909**  
BILLION

PENETRATION:  
**46%**

ACTIVE SOCIAL  
MEDIA USERS



**1.514**  
BILLION

PENETRATION:  
**36%**

MOBILE  
SUBSCRIPTIONS



**3.999**  
BILLION

vs. POPULATION:  
**96%**

ACTIVE MOBILE  
SOCIAL USERS



**1.441**  
BILLION

PENETRATION:  
**35%**

we  
are  
social



we  
are  
social

JAN  
2019

# PAKISTAN

THE ESSENTIAL HEADLINE DATA YOU NEED TO UNDERSTAND MOBILE, INTERNET, AND SOCIAL MEDIA USE



TOTAL  
POPULATION



**202.7**  
MILLION

URBANISATION:

**37%**

MOBILE  
SUBSCRIPTIONS



**154.3**  
MILLION

vs. POPULATION:

**76%**

INTERNET  
USERS



**44.61**  
MILLION

PENETRATION:

**22%**

ACTIVE SOCIAL  
MEDIA USERS



**37.00**  
MILLION

PENETRATION:

**18%**

MOBILE SOCIAL  
MEDIA USERS



**36.00**  
MILLION

PENETRATION:

**18%**



we  
are  
social



we  
are  
social

JAN  
2019

# ANNUAL DIGITAL GROWTH

THE YEAR-ON-YEAR CHANGE IN KEY STATISTICAL INDICATORS



TOTAL  
POPULATION



**+1.9%**

JAN 2018 – JAN 2019

**+4 MILLION**

MOBILE  
SUBSCRIPTIONS



**+5.6%**

JAN 2018 – JAN 2019

**+8 MILLION**

INTERNET  
USERS



**0%**

JAN 2018 – JAN 2019

**[UNCHANGED]**

ACTIVE SOCIAL  
MEDIA USERS



**+5.7%**

JAN 2018 – JAN 2019

**+2 MILLION**

MOBILE SOCIAL  
MEDIA USERS



**+13%**

JAN 2018 – JAN 2019

**+4 MILLION**



we  
are  
social



we  
are  
social

JAN  
2019

# DEVICE USAGE

PERCENTAGE OF THE ADULT POPULATION\* THAT USES EACH KIND OF DEVICE [SURVEY-BASED]



MOBILE PHONE  
(ANY TYPE)



82%

we  
are  
social

SMART  
PHONE



31%



LAPTOP OR DESKTOP  
COMPUTER



10%

we  
are  
social

TABLET  
DEVICE



1%

TELEVISION  
(ANY KIND)



76%



DEVICE FOR STREAMING  
INTERNET CONTENT TO TV



[N/A]

we  
are  
social

E-READER  
DEVICE



[N/A]



WEARABLE  
TECH DEVICE



1%

JAN  
2019

# FREQUENCY OF INTERNET USE

HOW OFTEN INTERNET USERS ACCESS THE INTERNET FOR PERSONAL REASONS (ANY DEVICE)



EVERY  
DAY



58%

AT LEAST ONCE  
PER WEEK



31%

AT LEAST ONCE  
PER MONTH



8%

LESS THAN ONCE  
PER MONTH



3%

we  
are  
social



JAN  
2019

# MOBILE CONNECTIONS BY TYPE

BASED ON THE NUMBER OF CELLULAR CONNECTIONS (NOTE: NOT UNIQUE INDIVIDUALS)



TOTAL NUMBER  
OF MOBILE  
CONNECTIONS



**154.3**  
MILLION

we  
are  
social

MOBILE CONNECTIONS  
AS A PERCENTAGE OF  
TOTAL POPULATION



**76%**

GSMA

PERCENTAGE OF  
MOBILE CONNECTIONS  
THAT ARE PRE-PAID



**96%**

GSMA

PERCENTAGE OF  
MOBILE CONNECTIONS  
THAT ARE POST-PAID



**4%**

GSMA

PERCENTAGE OF MOBILE  
CONNECTIONS THAT ARE  
BROADBAND (3G & 4G)



**41%**

APR  
2019

# SHARE OF MOBILE WEB TRAFFIC BY MOBILE OS

BASED ON EACH OPERATING SYSTEM'S SHARE OF GLOBAL MOBILE WEB REQUESTS

PERCENTAGE OF MOBILE  
WEB REQUESTS FROM  
ANDROID DEVICES



**75.3%**

PERCENTAGE OF MOBILE  
WEB REQUESTS FROM  
APPLE IOS DEVICES



**22.4%**

PERCENTAGE OF MOBILE  
WEB REQUESTS FROM OTHER  
MOBILE OPERATING SYSTEMS



**2.3%**

we  
are  
social





JAN  
2019

# FINANCIAL INCLUSION FACTORS

PERCENTAGE OF THE POPULATION AGED 15+ THAT REPORTS OWNING OR USING EACH FINANCIAL PRODUCT OR SERVICE



HAS AN ACCOUNT WITH  
A FINANCIAL INSTITUTION



we  
are  
social

21%

HAS A  
CREDIT CARD



1.0%

HAS A MOBILE  
MONEY ACCOUNT



we  
are  
social

6.9%

MAKES ONLINE PURCHASES  
AND / OR PAYS BILLS ONLINE



8.0%

PERCENTAGE OF WOMEN  
WITH A CREDIT CARD



0.7%

PERCENTAGE OF MEN  
WITH A CREDIT CARD



we  
are  
social

1.2%

PERCENTAGE OF WOMEN  
MAKING ONLINE TRANSACTIONS



3.3%

PERCENTAGE OF MEN  
MAKING ONLINE TRANSACTIONS



12%

APR  
2019

# SOCIAL MEDIA ADVERTISING AUDIENCES

A COMPARISON OF THE TOTAL ADDRESSABLE ADVERTISING AUDIENCES\* OF SELECTED SOCIAL MEDIA PLATFORMS

 CHANGES IN DATA PROVIDER METHODOLOGIES MEAN THAT DATA ON THIS SLIDE IS NOT DIRECTLY COMPARABLE TO DATA IN OUR PREVIOUS REPORTS

POTENTIAL REACH  
OF ADVERTISING  
ON FACEBOOK



**1,887**  
MILLION

FEMALE: **43%**  
MALE: **57%**

POTENTIAL REACH  
OF ADVERTISING  
ON INSTAGRAM



**802**  
MILLION

FEMALE: **52%**  
MALE: **48%**

POTENTIAL REACH  
OF ADVERTISING  
ON TWITTER



**262**  
MILLION

FEMALE: **34%**  
MALE: **66%**

POTENTIAL REACH  
OF ADVERTISING  
ON SNAPCHAT



**311**  
MILLION

FEMALE: **61%**  
MALE: **38%**

POTENTIAL REACH  
OF ADVERTISING  
ON LINKEDIN



**615**  
MILLION

FEMALE: **43%**  
MALE: **57%**



we  
are  
social



we  
are  
social

# Technology Changed / Shape our Life

sheeps\_sell Instagram



Yes, in Kuwait they sell sheeps on Instagram!!!

145 likes 13 comments





UBER

World's largest  
taxi company

Owens NO

~~Taxis~~



World's largest  
Accommodation provider

Owens NO

~~Real  
estate~~



World's largest  
Phone companies

Owens NO

~~Telco  
infra~~



Alibaba Group

World's most  
Valuable retailer

Owens NO

~~Inventory~~

facebook.

Most popular  
Media owner

Owens NO

~~Content~~



World's fastest  
Growing bank

Owens NO

~~Actual  
money~~

NETFLIX

World's largest  
movie house

Owens NO

~~Cinemas~~



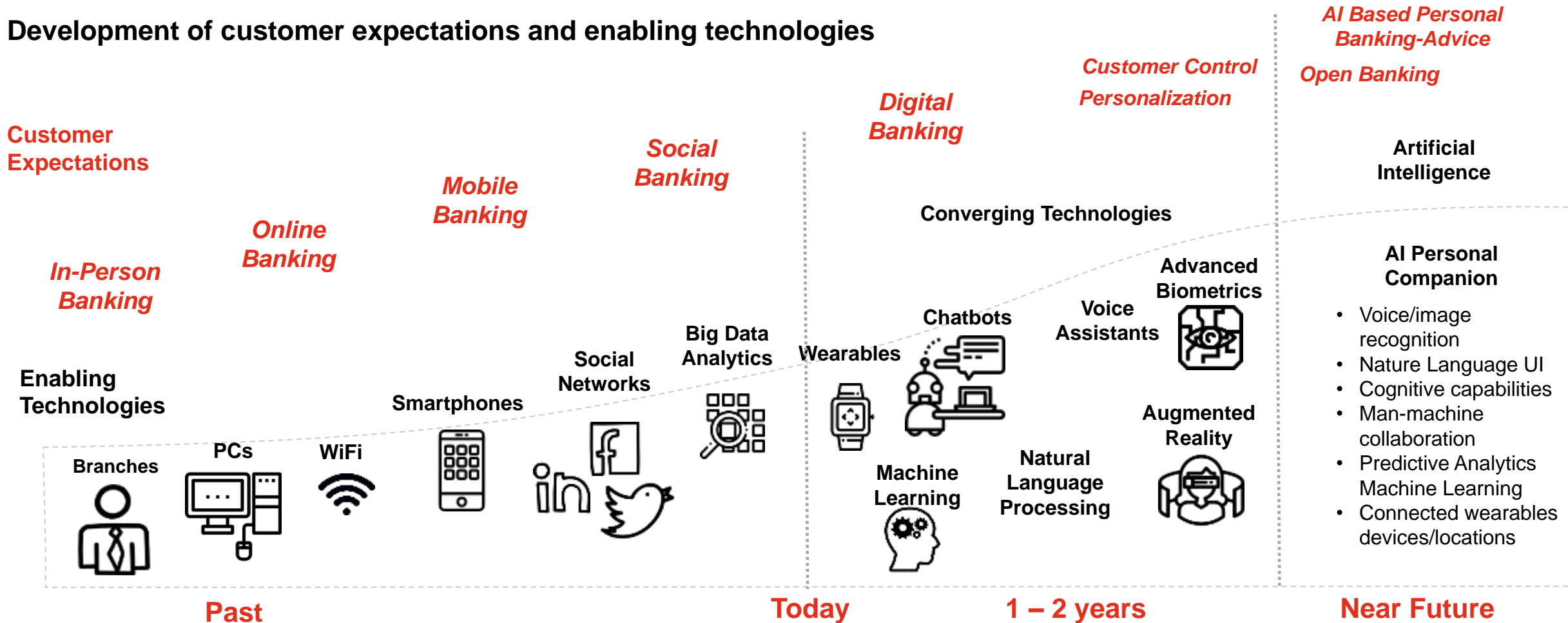
World's largest  
Software vendors

Owens NO

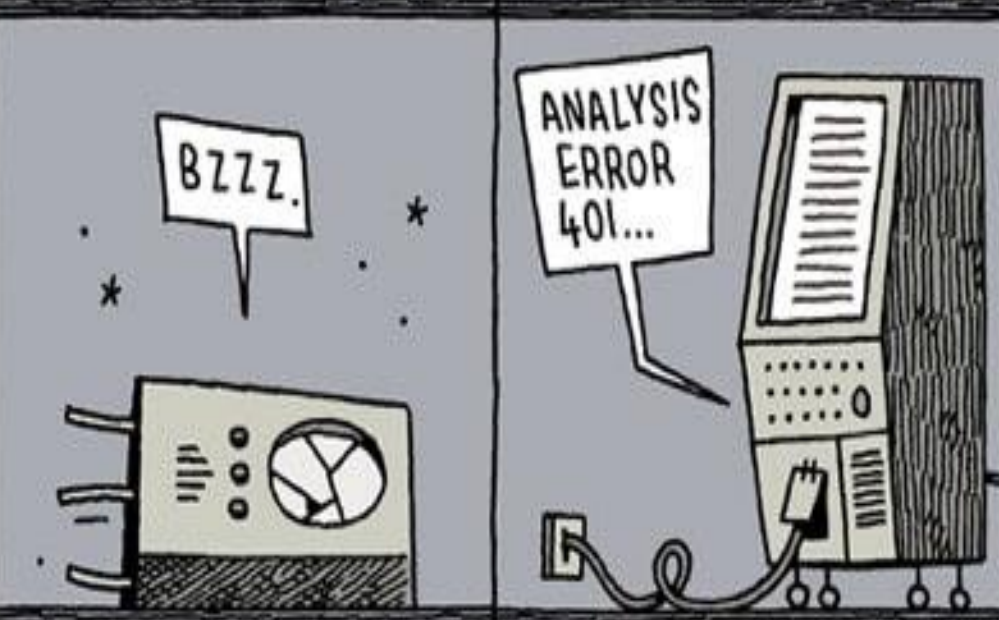
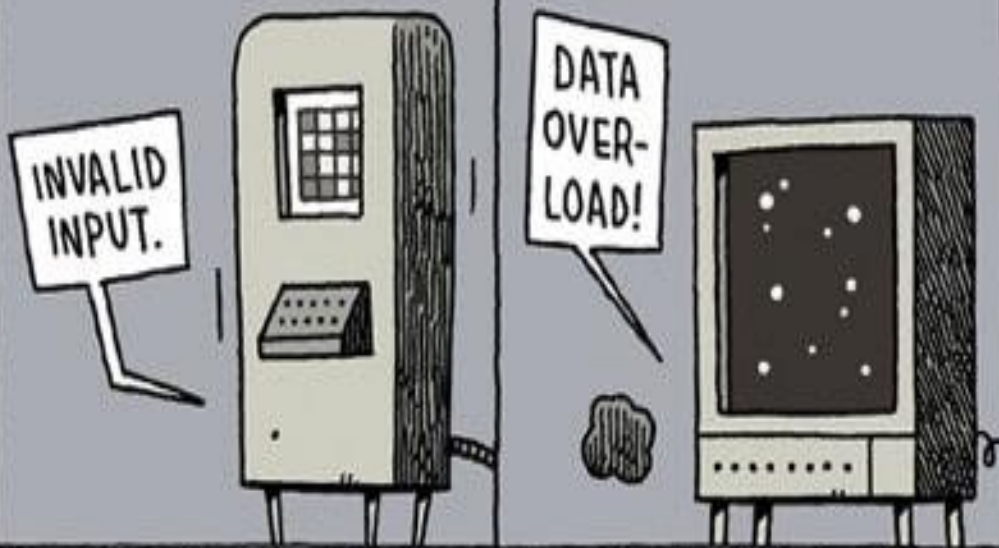
~~Apps~~

# AI and Machine Learning to reshape how banks do business

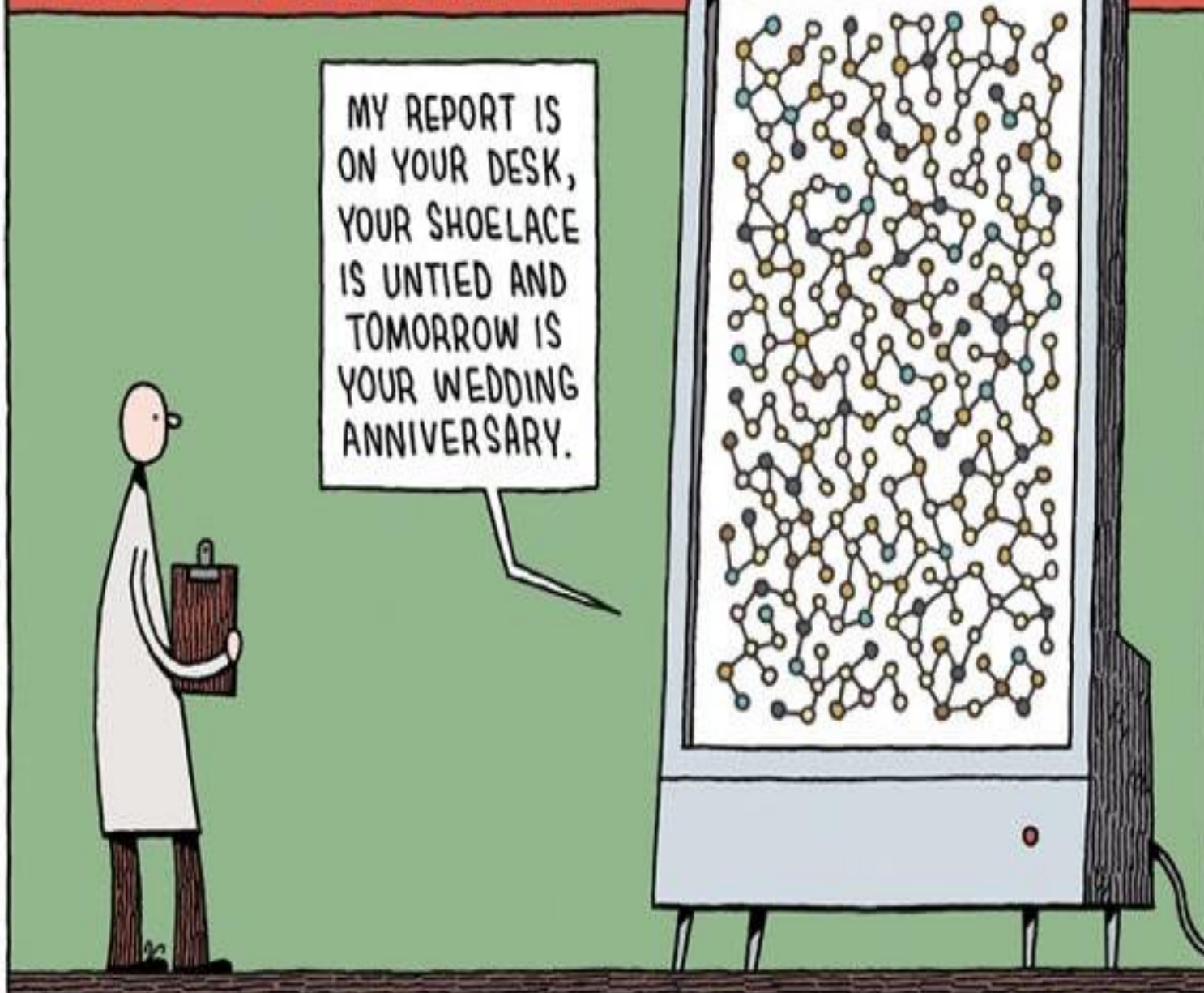
Development of customer expectations and enabling technologies



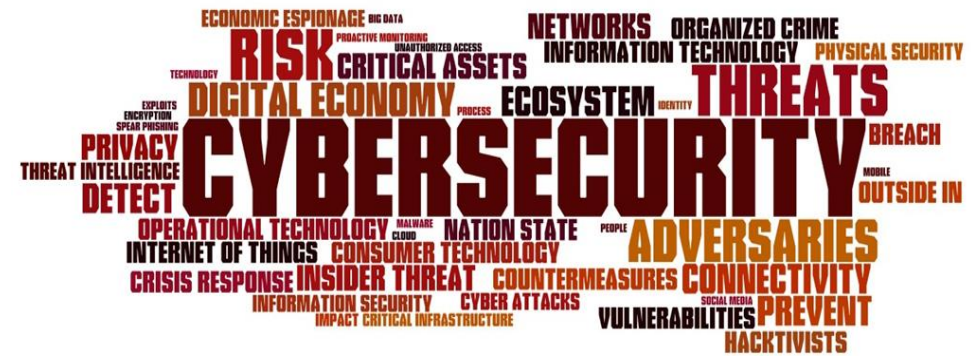
# A.I. of the PAST...



# A.I. of TOMORROW...



## Cyber Security



Increased use of information technology means greater exposure to cyber attacks

---

## *Cyber Security*

The More we're Dependent on  
technology,  
the More we're vulnerable





## *Cyber Security*

*Employees are responsible for 27% of all cyber security incidents*



Source: PwC GSISS 2018

## Cyber Security



## ***Why is cybersecurity Important ?***

- ✓ ***Cyber security*** risks are now ***commanding Top level attention*** as businesses are transformed by digital technologies.
- ✓ Shared responsibility that requires ***cross functional disciplines***.

## ***What valuable assets do I have?***

**MONEY**

**Information**

**Critical  
Service**

- **The global threat is increasing**
  - ✓ **Every Minute 1 website has been hacked**
  - ✓ **Every Minute 450 attacks in the world (36% more than 2017)**
  - ✓ **Every Day 300,000 Social Media accounts compromised**
  - ✓ **Every Day 200,000 Viruses are generated**
  - ✓ **Every Day 1.9 Million Records compromised**

***No longer just an IT challenge  
but a priority issue for ALL***

# Cyberattacks are headline news everyday

**THE WALL STREET JOURNAL.**  
Global Finance: Data Breach To Cost Card Processor

Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies

**POLITICO**  
...onsidering cybersecurity incentives

**THE WALL STREET JOURNAL.**  
U.S. Charges Snowden in Security-Leak Case

Hackers steal £650 million in world's biggest bank raid

**REUTERS**  
EU could make firms disclose network security breaches

Obama executive order seeks better defense against cyber attacks

**Obama to confront Chinese president over spate of cyber-attacks on US**  
US president to meet with Xi Jinping over latest allegation that Chinese hackers gained access to US weapons systems

**REUTERS**  
Cyber attacks on Gulf infrastructure seen rising

**Kaspersky Lab sees rise in 'hacktivism,' state-sponsored cyber attacks in 2013**  
1210 words  
7 January 2013

**The New York Times**  
In Hours, Thieves Took \$45 Million in A.T.M. Scheme

Qatar National Bank hit by a cyber attack

**Cyberspace the new frontier in Iran's war with foes**  
1129 words  
24 October 2012

Sunday Main Book - News  
**China telecoms giant could be cyber-security risk to Britain**  
James Cusick

Latest waves of cyber attacks targeting US corporations

**Quick Heal Malware Report: Cyber attacks looming over India**  
391 words  
3 January 2013

**UK to set up "Cyber Reserve" force to counter cyber crime**  
Distributed by Comfy.com  
551 words  
4 December 2012

**Brave new world of multi- phase cyber attacks looms**  
Christopher Joye  
1085 words  
9 January 2013  
The Australian Financial Review

**THE WALL STREET JOURNAL.**  
Iran Blamed for Cyberattacks --- U.S. Officials Say Iranian Hackers Behind Electronic Assaults on U.S. Banks, Foreign Energy Firms

## propakistani

**Hackers Steal Money from Standard Chartered Accounts by Hacking ATMs**

**BankIslami Customers Lose Over \$6 Million in Biggest Security Breach in Pakistan's History**

**DISCLAIMER**  
All news have been taken from public domain so no claim is made for accuracy, completeness, or adequacy of the information are made.

**Pakistani Hackers Involved in \$81 Million Bangladesh Bank Heist**

**Habib Bank Gets Hacked, Databases Leaked Online!**

**Hackers Steal Money from Faysal Bank Customers Once Again!**

# Cyberattacks are headline news everyday



**THE VERGE**  
TRENDING NOW  
LG is spending tons on the headphone bet  
iPhone 7 rumored to include pressure sensor

LONGFORM... PREVIEWS... VIDEO... TECH... CIRCUIT BREAK... SCIENCE... ENTERTAINMENT... CRIS... TLDR

PREVIOUS STORY  
This may also could be the future of robot vision

## Delta flights delayed worldwide due to 'computer outage'

By Jerome Whelan on August 8, 2016 at 10:45 AM

Introducing TOU  
Get up to 20% savings on  
Hertz  
Book now

**DELTA**

187	DELTA	7:13 AM	C61	On Time
583	DELTA	8:25 AM	C54	On Time
419	DELTA	9:47 AM	C55	Now At 12:15 PM
14	DELTA	6:37 AM	C52	Now At 8:30 AM
362	DELTA	6:15 AM	C53	Now At 8:30 AM
378	DELTA	7:58 AM	C52	Now At 9:48 AM
741	DELTA	10:05 AM	C52	Now At 11:30 AM
370	DELTA	6:30 AM	C56	Now At 8:45 AM
327	DELTA			
354	DELTA			
489	DELTA			
303	DELTA			
310	DELTA			
295	DELTA			
304	DELTA			

**Millions of \$\$\$ losses...**

**Hundreds of flights canceled...**

**Thousands of passengers stranded**

# A World of Targets with Increased Value

## 4 Billion Users Online

Up from 2+ Billion today

## 25+ Million Applications

Connected and Creating 50x the volume of data

## 50 Trillion Gigabytes

Amount of data being created per year

## 50-200 Billion Devices

Connected to the Internet

## 400k New Malware/Day

630 million unique samples of malware exist today

## \$6 trillion

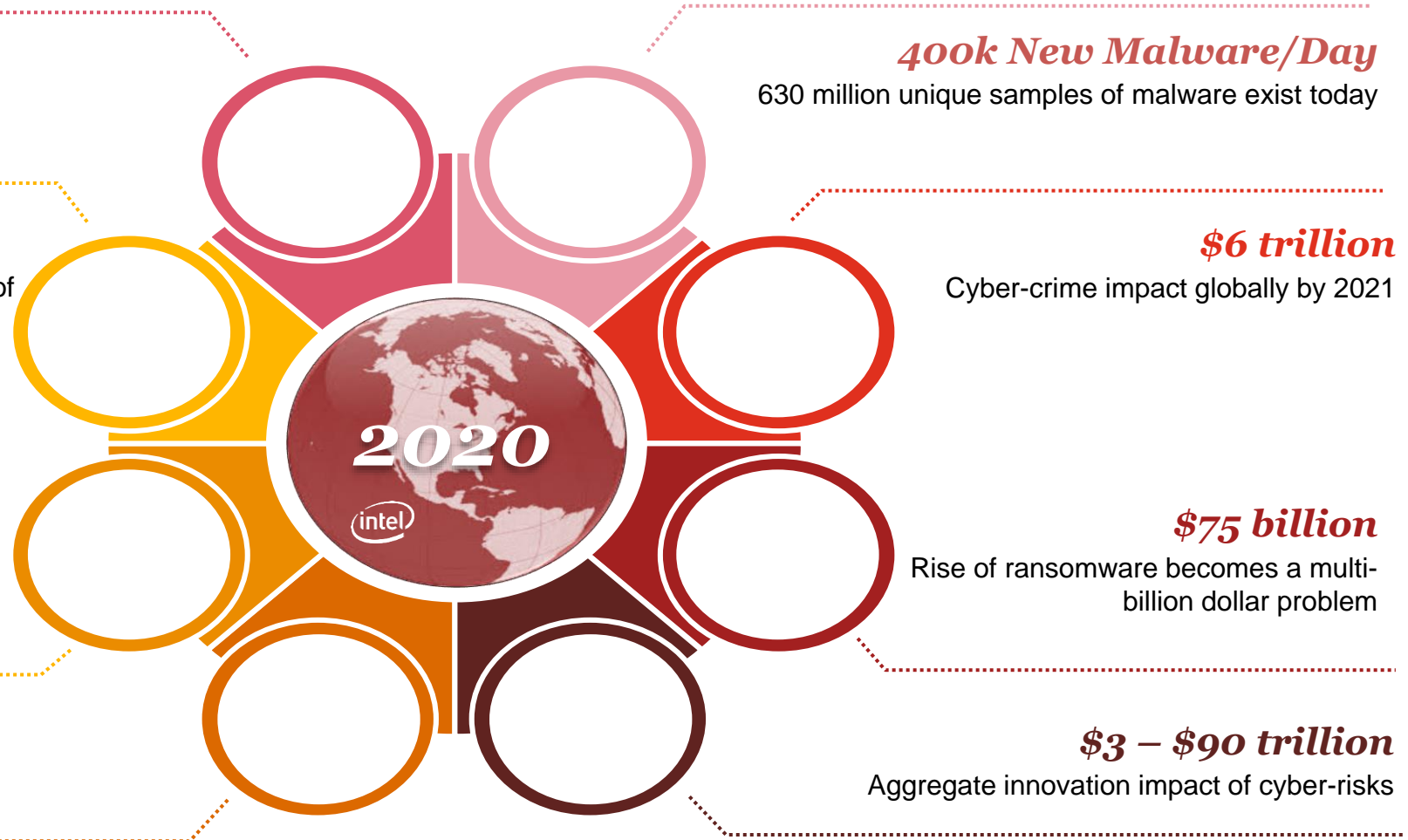
Cyber-crime impact globally by 2021

## \$75 billion

Rise of ransomware becomes a multi-billion dollar problem

## \$3 – \$90 trillion

Aggregate innovation impact of cyber-risks



***The STAKES are HIGH !!!!!***

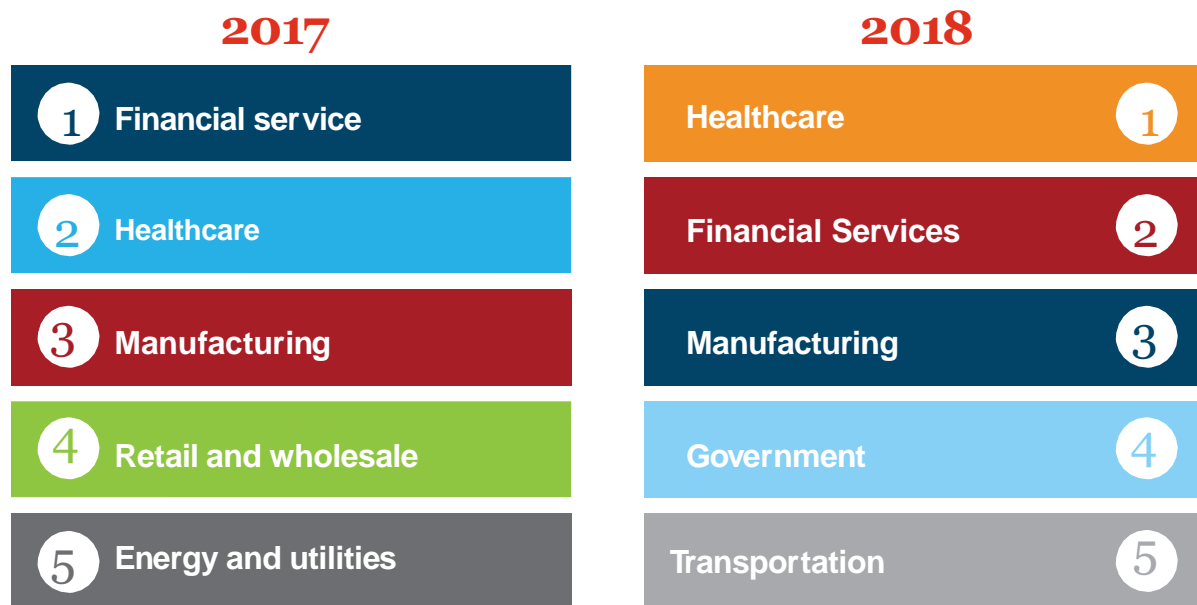


***“Cybersecurity is no longer just about deflecting attackers.***

***Today, it's about figuring out how to manage and stay ahead of intruders who are already inside the organization”***



# The 5 Most Cyber Attacked Industries



### Cyber Crime Rates – Dark Web

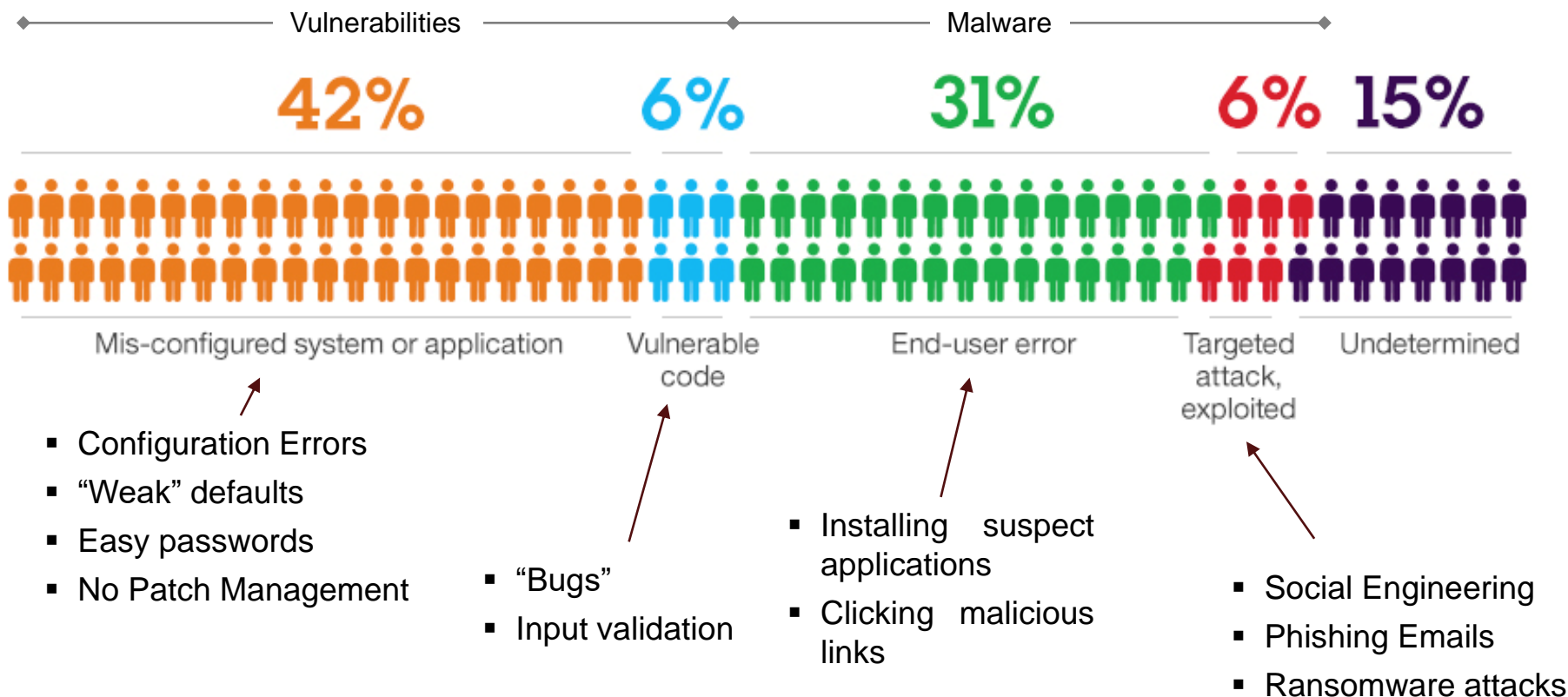
- Corporate mailbox hack \$500
- Private mailbox hack \$129
- Credit card number \$7
- Premium credit card \$80



**The average cost of managing and mitigating breaches rose to \$3.1 million per incident in 2017, three times than in 2016**

(2017 IBM Cyber Intelligence Index Survey)

# Why do Breaches Happen ?



**57%** of Boards have no mechanism to **measure security effectiveness**

**1 in 4 Companies** fails to conduct Cyber Security Risk Assessment due to lack of resources and expertise.

**67%** are insiders **59%** of ex-employees admitted to stealing company data when leaving jobs.

# 2018 IN A NUTSHELL

**RANSOMWARE GOES MAINSTREAM**



**ENCRYPTION DEBATE**



**BANKS ATTACKED FROM WITHIN**



**DATA BREACHES**



**DDOS ATTACKS TAKEN TO THE NEXT LEVEL**



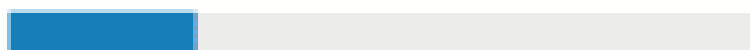
**INFORMATION WARFARE?**

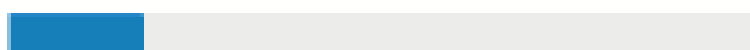


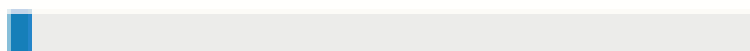


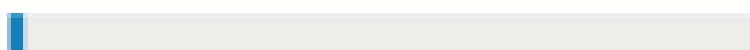
## Who's behind the breaches?

**75%**   
perpetrated by outsiders.

**25%**   
involved internal actors.

**18%**   
conducted by state-affiliated actors.


**3%**   
featured multiple parties.

**2%**   
involved partners.


**51%**   
involved organized criminal groups.



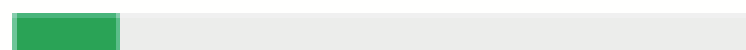
## What tactics do they use?

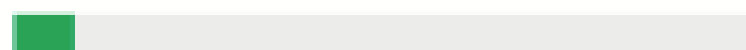
**62%**   
of breaches featured hacking.

**51%**   
over half of breaches included malware.






**81%**   
of hacking-related breaches leveraged either stolen and/or weak passwords.

**43%**   
were social attacks.

**14%**   
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

**8%**   
Physical actions were present in 8% of breaches.

# Global Cyber Security Breaches

<p><b>Key cyber threat scenario</b></p>	 <p><b>Banking System infiltrated by the hackers</b></p>	 <p><b>Leak of sensitive information by APT attack</b></p>	 <p><b>Ransomware attack targeting users</b></p>
<p><b>Typical threat actors</b></p>	<p>Organized Crime, Hackers, hackers</p>	<p>Hackers, hacktivists, chancers</p>	<p>Organised Crime, Nation states</p>
<p><b>Primary Motivations</b></p>	<p>Financial Gain</p>	<p>Financial Gain, Identity Theft</p>	<p>Financial gain, espionage</p>
<p><b>Recent example</b></p>	 <p><b>Bangladesh Central Bank</b></p> <p><b>A Bangladeshi central bank official's computer was used by unidentified hackers to make payments via SWIFT. Most of the transfers were blocked but about \$81 million was sent to multiples banks out of country</b></p>	 <p><b>In 2016, Yahoo announced that hackers have stolen 3 billion user account details resulting decline in stock price.</b></p>	<p><b>150 Countries</b></p> <p><b>On May 12 a strain of ransomware called WannaCry spread around the world, walloping hundreds of thousands of targets, including public utilities and large corporations, NHS hospitals and facilities in UK</b></p>

# Global Cyber Security Breaches

**Key cyber threat scenario**



**Malware attack targeting critical IT Infrastructure**



**Infiltrate using phishing email containing sophisticated malware.**



**Malware attack targeting critical IT Databases**

**Typical threat actors**

Organised Crime, Nation states

Nation states

Organised criminals, Hackers

**Primary Motivations**

Financial Gain, Espionage

Financial gain, competitive advantage, espionage

Financial Gain, Identity Theft

**Recent example**

**Aramco**

***In 2012, In a matter of hours, 35,000 computers were partially wiped or totally destroyed. Saudi Aramco's ability to supply 10% of the world's oil was suddenly at risk.***



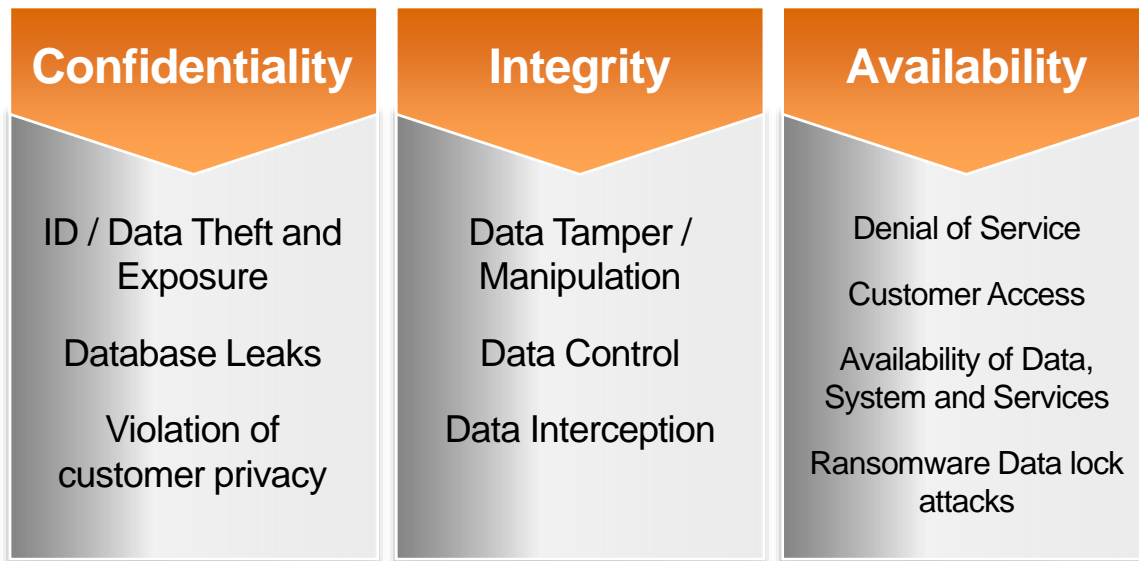
***Hackers breached health care insurance provider affecting record of 78.8 million users, costing damages worth minimum (\$115 million)***



***More than 11 million healthcare policyholder accounts were possibly compromised when criminals used a 'developer' computer to access sensitive database, costing approx \$10 million.***

## *What is Cyber Security ?*

Cyber Security is a set of principles and practices designed to safeguard your computing assets and online information against threats.



*Think*

***BIG!!!***

## ***Most Common Cyber Security Attacks***

<b>Hacking</b>	Illegal Intrusion into a computer system or network with(out) destructive motives / intention.
<b>Ethical Hacking</b>	Legal intrusion into a computer system or network with motive of discovering weaknesses and loopholes in the system.
<b>Cyber Crime</b>	Computer used as an object or subject of crime.
<b>SPAM</b>	Programs designed to send a message to multiple users, mailing lists or email groups
<b>Zero Day Exploits</b>	An unknown vulnerability in an information system.
<b>Malware</b>	Botnets, Backdoors and Key Loggers
<b>Identity Theft</b>	Stole your ID and Important Information to commit fraud
<b>Denial of Service Attack</b>	Attempts to flood a network to disrupt the service / emails and prevent accessing it.



## Most Common Cyber Security Attacks

# RANSOMWARE : THREAT TO BUSINESS

Ransomware is serious threat to business, it is a special kind of virus used by hackers to lock access to important files on user's computers; and they ask for money (ransom as they've virtually kidnapped the files) to unlock the files again. Imagine that you have important client files to be delivered and they just got locked by Ransomware - *I know your heart skipped a beat..*

### HOW YOU GET INFECTED



Virus delivered as email attachment OR embedded link.



Visiting infected websites which deliver malware automatically.



Using Unknown USB Drives - they may contain malware.

- 300,000 Systems
- 150 Countries
- Payment via Bitcoin
- Lateral Movement

### Impacts

- UK 20 Hospitals
- Spain / Portugal (Telecom)
- Russian (Banking)
- Germany (Railway)
- US – FADEX
- China – Universities
- Japan - 600 Companies

## *Most Common Cyber Security Attacks*



Scams involve an attacker masquerading as a trusted person using real credentials to infiltrate an organization's computer system.

- Shoulder Surfing (Visual Hacking)
- Dumpster Diving
- Eavesdropping
- Persuasion
- Online Communication

# Phishing

**RE: INSTRUCTION TO TRANSFER OVER DUE PAYMENT OF \$5.8M**  
 From: Rev.Lee Johnson [Add to Contacts](#)  
 Sent: Mon, Apr 18, 2016 at 4:38 pm  
 To: Recipients

INTERNATIONAL FINANCE CORPORATION.  
 LEICESTER CURRENCY  
 CHEQUE/DRAFT DEPARTMENT  
 TELEGRAM: FBNFOREX

RE: INSTRUCTION TO TRANSFER OVER DUE PAYMENT OF \$5.8M

ATTENTION:

This is to inform you that this office received payment advice from The Corporation (INPC) in conjunction with the Ministry of Finance of the to you the total amount of US\$5.8 Million. Note that a final approval your funds have been transferred from the International Finance Corporation final authority to transfer out of the shores such amount of Fund.

We have just received an email from one MR. KAMICHI \*\*\*\*\* who introduced that you have instructed him to receive the funds into his account on informed us that you are dead also that the instruction was given to him him to forward the copy of the letter you gave him but have not yet he


**THIS IS THE ACCOUNT DETAILS HE FORWARDED TO US:**  
 Bank Name: MIZUHO BANK, NARIMASU BRANCH.  
 Address: 2-11-2, NARIMASU, ITABASHI-KU, TOKYO, JAPAN  
 SWIFT CODE: MSDKDBGHUT. Bank Account No: 239-1-563-321.  
 Beneficiary: ROS LTD. (KAMICHI BLAKE)

We are writing you to confirm this message and if it is not true, you notifying us of the need to rectify this fallacy. Please note that a would be required to ascertain the authenticity of your claim. This off details on how to obtain the transfer Authorization code which proves fund as we don't want the fund to get to the wrong hands. Since that it needs for the transfer of your fund to your designated bank account.

We await your urgent response.  
 Rev. Lee Johnson

---  
 This email has been checked for viruses by Avast antivirus software.  
<https://www.avast.com/antivirus>

**Your Bank Of America Security Update**  
 From: Bank Of America [Add to Contacts](#)  
 Sent: Fri, Mar 11, 2016 at 3:07 pm  
 To: Recipients



**Activity Alert**  
 PERSONAL CHECKING/SAVINGS ACCOUNT  
**IP-Conflict detected on your account**

Dear Customer,

g you know that we've detected multiple IP-Conflict on your online account. result to restrictions and closure of your online account. Kindly verify your low to ensure the safety of your assets and online account.

tion click **SIGN ON** to restore and ensure the safety of your Account .

**Security Checkpoint**

From the authenticity of messages from us, always look for this Security point. You last signed in to Online Banking on 18/02/2016.


**ber:** Always look for your SiteKey@ before entering your Passcode. We'll ask your Online ID and Passcode when you sign in.

vice email from Bank of America. Please note that you may receive service emails in with your Bank of America service agreements, whether or not you elect to receive email.


vacancy Notice.

reply directly to this automatically generated email message.

merica Email, 8th Floor-NC1-002-08-25, 101 South Tryon St., Charlotte, NC 28255-0001

merica, N.A. Member FDIC. Equal Housing Lender   
 Bank of America Corporation. All rights reserved.

**Suspicious Activity On Your Online Account**  
 From: Chase Online [Add to Contacts](#)  
 Sent: Thu, Apr 21, 2016 at 3:18 pm  
 To: wait\_turner@securewebapps.com



**Account Suspension**

We are writing to inform you about the suspension of your account, a series of suspicious activities are detected in your account by our monitoring system. This is a precautionary step taken by our monitoring systems to try and catch fraudulent activities before they happen.

**Possible events occurred**

1. Log in attempts from an unusual or unrecognized device or location.
2. Too many incorrect log in attempts.
3. Requesting any banking operation using unusual pattern.

To enable your account you will have to authenticate your identity so that all the limitations from your account can be removed.

[Confirm now](#)

Thank you,  
 Chase

Date: 05-10-2016

Member FDIC | Equal Housing Lender

"Chase," "JPMorgan," "JPMorgan Chase," the JPMorgan Chase logo and the Octagon Symbol are trademarks of JPMorgan Chase & Co.  
 © 2016 JPMorgan Chase & Co.

## *Vishing - Video*



**WATCH THIS HACKER  
BREAK INTO  
MY CELL PHONE ACCOUNT  
IN 2 MINUTES**

## *The Hacker's / Bad Actors Objectives*

- **Denial of data access** (blocking someone from accessing a storage device).
- **Intellectual Property (IP) theft** (stealing the top secret formula for a soft drink).
- **Inflicting loss of reputation** through exposure of sensitive information (revealing a political candidate's tax returns or medical records).
- Creating **loss of trust** in a corporation (exposing a bank or credit card institution's security weakness).
- **Extortion** (demanding a ransom payment in return for restoring one's data access or keeping sensitive data from becoming public).
- **Kinetic effect** (having something happen in the real world—such as shutting off a power grid, controlling a patient drug infusion device, or controlling an airplane).

# Insider Threats

An insider threat is the threat posed by an employee, contractor, or other person who has access to a company’s information and systems.

- Working Odd Hours
- Unauthorized Removal
- Seeking Info
- Unauthorized Devices
- Foreign / Domestic Travel
- Unreported Contacts
- Bragging
- Disgruntlement
- Unexplained Affluence
- Unnecessary Copying

## How to Effectively Manage Insider Threats



# *What's the impact of a cyber attack? Security Compliance Drivers*

## **Direct Costs**

*Investigation & Remediation*

*Regulatory Sanctions/penalties*

*Customer Redress*

## **Indirect Costs**

*Increased Cyber Insurance Premium*

*Customer Fraud/ write offs*

*Class Action Law Suit*

## **Intangible Costs**

*Damage to Brand*

*Heads Roll*

*Competitive Disadvantage*

# *What are Organisations thinking about?*



## **1. Protecting Assets**

- Cybersecurity
- Data Breaches
- Data Privacy Protection



## **2. Innovation**

- Data driven decisions
- Engaging Business Partners
- Targeting Masses



## **3. Continuous Improvement**

- Improve Productivity
- Minimize Losses
- Scalability & Flexibility



# IT / IS Regulations and Circulars in Pakistan

**Digital  
revolution**



**Growing  
cyber risk**



**More  
regulation**

## State Bank of Pakistan

- ✓ Guidelines on Business Continuity Planning
- ✓ Information Technology Security
- ✓ IS Guidelines on audits and system switchover
- ✓ Prevention against Cyber Attack

- ✓ Security of Internet Banking – PSD
- ✓ Payment Card Security – PSD
- ✓ Outsourcing of IT Services
- ✓ Security of Digital Payments – PSD
- ✓ Few in Draft Stages

### *Prevention of Electronic Crime Act -2016*

- ✓ Unauthorized access to information system and data
- ✓ Unauthorized copying or transmission of data
- ✓ Cyber terrorism
- ✓ Electronic forgery
- ✓ Electronic fraud
- ✓ Tampering etc. of communication equipment
- ✓ Unauthorized interception
- ✓ Malicious code
- ✓ Spamming
- ✓ Spoofing

## Enterprise Technology Governance and Risk Management Framework

### Other Countries

- Bangladesh
- EU
- France
- Germany
- India
- Ireland
- Israel
- Malaysia
- Saudi Arabia
- Singapore
- South Africa
- USA

# Synopsis of SECP's Directive on Cyber-Security Framework



## Framework

- Continuous
- Proactive
- Predictive
- Adaptive
- Distil key lessons
- Monitor developments
- User Metrics based maturity assessment

## ***SEC Directive on Cybersecurity Framework for Insurance Sector 2019***

- 1. Developing cybersecurity framework and mechanisms***
- 2. Alignment of Cybersecurity Framework with overall Risk Management Framework***
- 3. Appointment of Chief Information Security Officer (CISO)***
- 4. Insurers to conduct cybersecurity framework and risk assessment***
- 5. Regulatory Reporting***
- 6. Data Security and Confidentiality***
- 7. Insurers to obtain cyber risk insurance***
- 8. Insurers to have adequate cybersecurity systems in place***
- 9. The Cybersecurity Framework for Insurance Sector***

## ***Summary - Directive on Cyber- Security Framework for Insurer(s)***

- ✓ The Security and Exchange Commission of Pakistan has proposed Directive on **8<sup>th</sup> January, 2019** under section 12 of the **Insurance Ordinance, 2000**. Suggestions in **14 days**.
- ✓ The Directive will be effective from **1<sup>st</sup> March, 2019 (still under discussion)**
- ✓ The framework will **apply to all Life and non-Life Insurers** including family and general takaful operators.
- ✓ Accordingly, the Insurer(s) have been required to **upgrade their systems, controls and procedures**.
- ✓ The framework is **not "one-size-fits-all"** and implementation of the same shall be risk-based and commensurate with **size, nature and types of products and services and complexity of Technology Infrastructure, network operations, delivery channels** of the Insurer(s).
- ✓ Framework is being enhanced with **extensive consultation** with both internal & external stakeholders and will serve as **baseline requirement** for all Insurers(s)
- ✓ Cybersecurity decision requires a very wide spectrum of involvement - **from corporate governance down to penetration testing and vulnerability analysis**.
- ✓ Framework is based on **principles of international standards and best practices** for cyber security and cyber-risk management. It aims to provide enabling regulatory environment for managing risks associated with the use of technology.

## ***Summary - Directive on Cyber- Security Framework for Insurer(s)***

- ✓ SECP encourages Insurer(s) to form cybersecurity framework and consider collection of standards and best practices. These include **NIST Cybersecurity Framework, ISO 27000 series and ISACA's CobIT**. SECP also encourages to consider **FSB - Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices**, and **IAIS** draft application paper focusing on **Supervision of Insurer's Cybersecurity**.
- ✓ SECP has further advised the Insurer(s) to follow a **phased approach towards implementation of the framework** starting with a **gap analysis** between their current status and this framework, **development/update** of the policy framework, on-the-ground **implementation and follow up review and feedback**.
- ✓ The Cyber-Security framework shall be **integrated and aligned** with the Insurer(s) **overall enterprise risk management program** and shall be approved by **Board**.
- ✓ **Appointment of CISO** as Senior Executive (Independent to IT) responsible for **implementation of cyber security framework** and report status to the Board **twice a year**.
- ✓ **Board** of Insurer shall be ultimate responsible for setting **strategy** and ensuring **cyber risk management**.
- ✓ While implementing this framework, **Insurer(s) are expected to exercise sound judgment** to determine the applicable provisions relevant to their **cyber risk profile**.

## ***Summary - Directive on Cyber- Security Framework for Insurer(s)***

### **Board Responsibility and Reporting**

- ✓ **Annually - Risk assessment program** on cybersecurity framework, risk acceptance criteria (RAC) and implementation measures. Justification shall be endorsed for overriding normal RAC.
- ✓ **Immediately – Significant changes** (Pre and Post Implementation) or any Cyber Incident

### **Commission / Regulatory Reporting**

- ✓ **Within 6 months** to this Directive – Submission of “Statement of Compliance”
- ✓ **Annually** (by April 30) – Compliance Statements and Cybersecurity framework assessment report signed off by CISO, CEO and independent auditor (if applicable)
- ✓ CISO shall make available to the Commission to explain steps taken after cybersecurity risk assessment.

### **Non-Compliance to this Directive**

- ✓ **Imposition of penalty** under section 40A of the SECP Act, 1997 - **10 million rupees or may extendable 100,000 rupees / day.**

## ***Summary - Directive on Cyber- Security Framework for Insurer(s)***

- ✓ Cyber security framework include **secure configuration** of hardware, operating systems, software, applications, databases and servers with **unnecessary services / programs disabled or removed**.
- ✓ Data security framework drives **insurer's responsibility** for safety and confidentiality of **policy holder data** including adoption of “**Prevention of Electronic Crimes act 2016**”.
- ✓ Data security framework shall ensure **encryption** at database level, storage level and during network transmission as per the **classification and sensitivity of the data** i.e. data at-rest, in-transit and in-storage.
- ✓ Data security framework includes protecting the policyholder data in the wake of **enhanced reliance on business process outsourcing (BPO), technology based agency arrangements and other strategic partnerships** for offering technology based innovative insurance products and services.
- ✓ In all arrangements (BPO, Agency, Strategic Partnerships etc.) the **privacy and fair usage of data clause** must be part of **SLA** between the insurer and the counterparty.
- ✓ All insurers and relevant business shall **only collect information necessary to provide insurance services** to the policyholder or potential policyholder through the technology based platforms.
- ✓ **Express consent of policy holder** shall be undertaken for full knowledge of **data collected, frequency, purpose** and further sharing with other party.

## ***Summary - Directive on Cyber- Security Framework for Insurer(s)***

- ✓ BoD / Sr. Management shall **cultivate awareness** and commitment to cybersecurity at all levels.
- ✓ All insurers should consider obtaining the **cyber risk insurance to cover their own cyber risks**, to which they are exposed, however effective system of controls remains the **primary defense** against cyber threats.
- ✓ Cyber Risk Insurance ideally cover against **Cyber extortion, Data Breach / Asset loss, Business Interruption.**
- ✓ Cyber insurance **coverage options** may be structured as **first-party (Direct Expenses) or third-party (by financial institutions)** coverage.
- ✓ Performing **proper due diligence** to understand available cyber insurance coverage such as **scope, terms, exclusions, not one-size fit all policy terms, impacts, financial strength, paying history** etc.)

**Overall Insurer should follow a Continuous Learning approach with review of cybersecurity strategy and framework and when events warrants, including its governance, risk and control assessment, monitoring, response, recovery, and information sharing components—to address changes in cyber risks, allocate resources, identify and remediate gaps, enhance user awareness and incorporate lessons learned.**



## ***Major Areas***

### ***SEC Directive on Cybersecurity Framework for Insurance Sector***

## ***The Cybersecurity Framework for Insurance Sector – Major Principles***

### **Cybersecurity Strategy and Framework**

- **Articulate principles - How Insurer intend to address cyber risks and strategy should be closely aligned with framework to achieve enterprise objective.**
- **Framework Objectives – Maintain and promote insurer’s ability for cyber incident response (Anticipate, detect, withstand, contain and recover), limit likelihood and impact.**
- **Cyber security Policy framework (Policies, Standards, Procedures)**
- **Cyber Security Infrastructure – People, Process and Technology**
- **Clearly defined roles and responsibilities / Organization Structure (BOD, Senior Management, Risk Management Committee, ITSC etc.)**
- **Alignment with Integrated enterprise risk management framework with consistency on all areas of risks such as Physical security, HR security etc.**
- **Cyber Security Risk Management (Identification of cyber security objectives and risk tolerance, mitigate and manage cyber risks associated with loss of CIA)**
- **Every risks shall be “owned” by a single name individual to ensure accountability.**
- **Regular review / update and monitoring of cyber security framework at defined frequency to remain effective.**
- **Threat Intelligence, Industry Collaboration and Situational awareness (proactive identification within the Insurer ecosystem)**

## ***The Cybersecurity Framework for Insurance Sector – Major Principles***

### **Risk and Control Assessment**

**The insurers shall identify functions, activities, products, and services—including interconnections, dependencies, and third parties—prioritize their relative importance, and assess their respective cyber risks,” and to “identify and implement controls—including systems, policies, procedures, and training—to protect against and manage those risks within RAC as set by BoD.**

- **Identification and classification of functions - Information assets and interconnections**
- **Prioritization of protection, detection, response and recovery efforts of insurer**
- **Inventory or mapping - Identification and maintenance of a current inventory or mapping of its information assets and system configurations. Risk assessment shall be performed and risk identified shall be managed i.e. reduction, acceptance, avoid or transfer.**
- **Identify dependencies according to asset classification and system configuration including 3rd party (vendors, cloud services providers, outsourced functions etc).**
- **Individual and system access rights management (access controls) – Need to know and Need to have.**
- **Integrate identification efforts with other processes such as systems acquisition, project management, change management, operations and delivery etc.**
- **Business Impact Analysis for identified cyber risks arising from both external and internal sources.**

## ***The Cybersecurity Framework for Insurance Sector – Major Principles***

### **Monitoring / Continuous Monitoring**

The insurers shall establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises.

Effective monitoring helps entities adhere to established risk tolerances and timely enhance or remediate weaknesses in existing controls,” and testing and auditing protocols provide essential assurance mechanisms.

- **Protect overall network (hardware, firmware and software components)**
- **Security Operations Centre (SOC)**
- **Early Detection and Containment**
- **Monitoring anomalous activities.**
- **Behavior / Signature based detection mechanisms**
- **Misuse of access including 3<sup>rd</sup> party and integrated with cyber threat intelligence program**
- **Identities and Credentials for physical, logical and remote access based on least privilege / SoD.**
- **Multi-layered detection controls – Defense in depth covering people, process and technology**
- **Effective intrusion detection capability – IDS / IPS / DLP / Event data aggregation**
- **Incident Response and Forensic Investigation – Ready Infrastructure**

## ***The Cybersecurity Framework for Insurance Sector – Major Principles***

### **Testing**

**Insurers shall rigorously tests all elements of their cybersecurity framework to determine their overall effectiveness before being employed within an insurer, and regularly thereafter.**

**The insurers shall consider using a combination of the available state-of-the-art testing methodologies and practices.**

**Currently, such state-of-the-art testing methodologies and practices, includes:**

- **Vulnerability Assessment**
- **Scenario- Based Testing**
- **Penetration Testing**
- **Red Team Test**
- **Response testing**
- **Integrated or Dynamic Testing**

# *The Cybersecurity Framework for Insurance Sector – Major Principles*

## **Response**

The insurers shall, in a timely manner,

- **assess the nature, scope, and impact of a cyber incident;**
- **contain the incident and mitigate its impact;**
- **notify internal and external stakeholders (such as law enforcement, regulators, and any other authorities, as well as shareholders, third-party service providers, and customers as appropriate); and**
- **coordinate joint response activities as needed.”**
  - **Awareness and Training**
  - **Investigation**
  - **Systems back up**
  - **Plan to resume critical operations**
  - **Access to external experts**
  - **Develop and test response, resumption, and recovery plans**
  - **System and process to support incident response**
  - **Responsible disclosure of potential vulnerabilities**
  - **Policy and procedure to meet the disclosure obligations**
  - **Forensic investigations**

# ***The Cybersecurity Framework for Insurance Sector – Major Principles***

## **Recovery**

The insurers shall be able to resume operations responsibly, while allowing for continued remediation, including by

- eliminating harmful remnants of the incident;
- restoring systems and data to normal and confirming normal state;
- identifying and mitigating all vulnerabilities that were exploited;
- remediating vulnerabilities to prevent similar incidents; and
- communicating appropriately internally and externally.

They shall consider the following while adopting recovery practices.

- Validated plans and procedures
- Timely recovery (such as “golden copy” of critical data)
- Review and improvement (Incident and Disaster Recovery)
- Contagion risk (propagation of malware or corrupted data due to 3<sup>rd</sup> party interconnection)
- Formal plans for communicating with all stakeholders.

## ***The Cybersecurity Framework for Insurance Sector – Major Principles***

### **Information Sharing**

- **Timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders.**
- **Cybersecurity information (i.e. threats and indicators, how vulnerabilities exploited, incidents, and responses) to enhance defenses, limit damage, increase situational awareness, and broaden learning.**

**The insurers may consider the following in respect of information sharing regarding cybersecurity.**

- (i) Information sharing (IRT based on joint efforts of Insurers)**
- (ii) Business-specific context (enhanced decision making)**
- (iii) Ability to understand threats posed by external service provider (Cyber threat intelligence operations)**
- (iv) Make cyber threat intelligence available to appropriate staff within the insurer having responsibility for the mitigation of cyber risks at the strategic, tactical, and operational levels.**



# *Way Forward / Action Plan*

## Today's Major Take Away ????

~~Secured By  
Design~~



## *How to Implement ????*



**1 in 4 Companies**

fails to conduct Cyber Security Risk Assessment due to lack of resources and expertise.

## **Action Plan / Way Forward**

### **1 – Implement Cyber Security Management Framework**

- ✓ **Establish appropriate cyber governance inc. senior sponsorship and board level MI**
- ✓ **Maintain a current asset inventory and identify crown jewels / critical assets, critical stakeholders.**
- ✓ **Conduct comprehensive risk assessment to determine Cyber Security capabilities, threats and weaknesses based on recognised framework (ISO, NIST etc.) and regularly assess against standard and regulatory requirements.**
- ✓ **Develop relevant policies, procedures, SOPs and templates.**
- ✓ **Implement internal assessment methods and ensure technical vulnerability assessment is performed quarterly and pen test annually**
- ✓ **Perform Business Impact Analysis and Develop detailed BCP / DRP with drills including ability to respond**
- ✓ **Implement automated solutions to monitor / track all types of Cyber attacks.**
- ✓ **Create and practice a broad cyber security incident response mechanism including security incident types, inventorize resources and assets, recovery plan hierarchy of communication flow, prepare variety of public statements**
- ✓ **Implement a probe the practices and procedures with respect to 3rd Party cybersecurity**

# Action Plan / Way Forward

## 2 – Implement Information Governance

- ✓ *Classify all documents with one of the four levels.*

**Highly Restricted** Most sensitive information with access controls, printing or re-distribution is locked

**Restricted** Majority of sensitive business and personal information with access controls, not shared unless approved

**Internal-Use Only** Proprietary information shared internally, not disclosed or available outside company  
*(Default setting)*

**Public** May be shared with public with approval prior to distribution

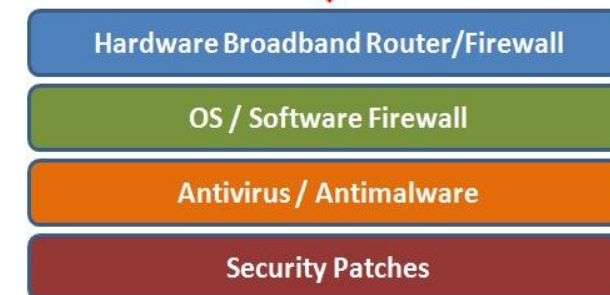
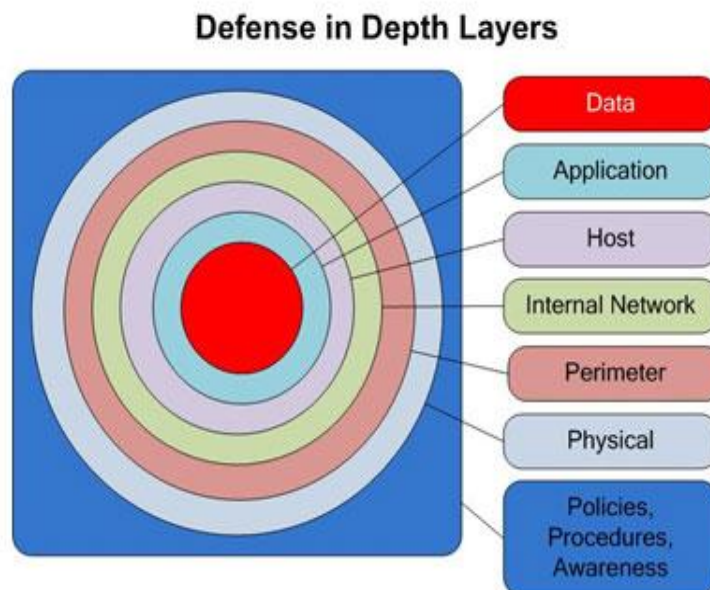
- ✓ *Enables uniform treatment of data by applying above level-specific controls*
- ✓ *Defines level of access controls and Identify who should have access including 3<sup>rd</sup> party.*
- ✓ *Encrypt critical Information assets and stored securely*



# Action Plan / Way Forward

## 3 – Implement Layered (Defense in Depth) Security

- ✓ *Incorporate a consistent and comparable approach for security controls selection.*
- ✓ *Implement Layered Security across organization (People, Process and Technology)*
- ✓ *Physical and Environmental controls*
- ✓ *Instrument your environment with effective detection and threat intelligence*
- ✓ *Having a Patching solution that covers your entire Infrastructure*



## ***Critical Security Controls***

- 1. Inventory of Authorized and Unauthorized Devices**
- 2. Inventory of Authorized and Unauthorized Software**
- 3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**
- 4. Continuous Vulnerability Assessment and Remediation**
- 5. Controlled Use of Administrative Privileges**
- 6. Maintenance, Monitoring, and Analysis of Audit Logs**
- 7. Email and Web Browser Protections**
- 8. Malware Defenses**
- 9. Limitation and Control of Network Ports, Protocols, and Services**
- 10. Data Recovery Capability**
- 11. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches**
- 12. Boundary Defense**
- 13. Data Protection**
- 14. Controlled Access Based on the Need to Know Basis**
- 15. Wireless Access Control**
- 16. Account Monitoring and Control**
- 17. Security Skills Assessment and Appropriate Training to Fill Gaps**
- 18. Application Software Security**
- 19. Incident Response and Management**
- 20. Penetration Tests and Red Team Exercises**

## Action Plan / Way Forward

### 4 – Security Awareness and Training

Your business is only as secure as its weakest link. Get comprehensive Cyber Security Awareness Training for your employees to avoid a possible breach.





# Action Plan / Way Forward

## 4 – Security Awareness and Training

Redefining Security Culture



- **Know your audience;** whether staff, vendors or customers.
- **Break down silos;** bring transparency to the security team.
- **Challenge assumptions and status quo;** why are we doing what we are doing?



- **Periodic and consistent security training** program – be deliberate
- **Measure progress**
- **Slow down the decision making** process – cold moments.



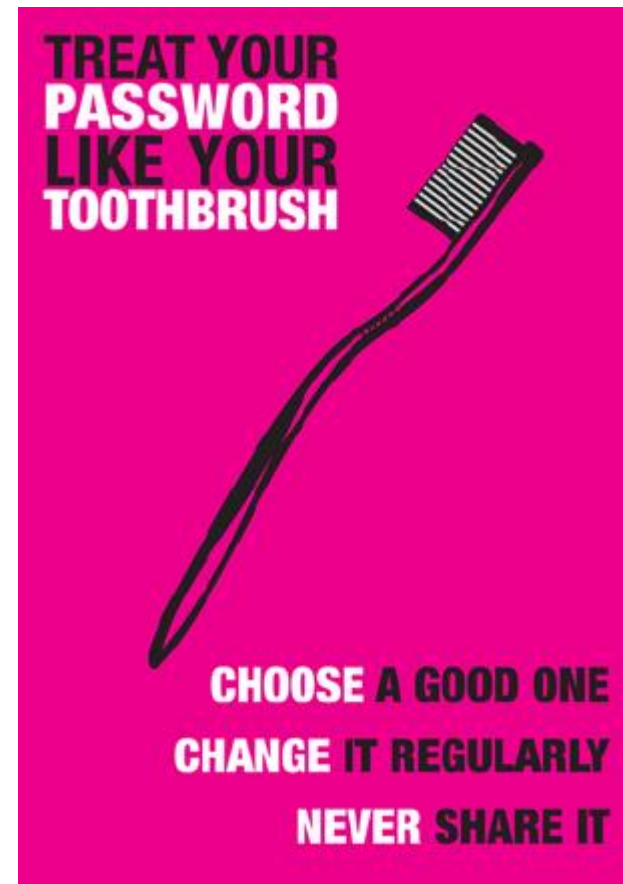
- **Make it personal** – use scenarios that don't only relate to office.
- Get senior **executives to lead by example** – walk the talk.
- **Big punishments vs small rewards.**

“Culture eats strategy for breakfast.”

- Peter Drucker

## ***Example – End User Awareness***

- Create and maintain strong password and passphrase.
- Avoid reusing the same password for multiple accounts.
- Do not use automatic logon functionality
- Secure your Mobiles with Pin Code.
- Secure your computer with Antivirus, Patches and update regularly.
- Protect the data you are handling and Backup Regularly.
- Assess risky behavior online and equip yourself with InfoSec knowledge.
- All “Company” correspondence should be sent from an official email address
- Avoid opening attachments / clicking on links from an untrusted source
- Avoid providing your user ID /password or any confidential information in an email or in a response to an email
- No use of Public WIFI



**STOP, and THINK, BEFORE you CLICK**

## *Action Plan / Way Forward*

### **5 – Cyber Insurance (Assessing the Exposure)**

- ✓ *To mitigate losses for malicious attacks, data breaches, business interruption and network failure*
- ✓ *Implementation of standards / best practices for basing premiums more coverage.*

### **6 – A Digital Forensics/Cyber Incident Response Firm on Call.**

- ✓ *Hire expert to investigate and create a defensible record if challenged later on (e.g. by regulators, user auditors, partners, customers, etc.)*

### **7 – Logging and Monitoring Capabilities.**

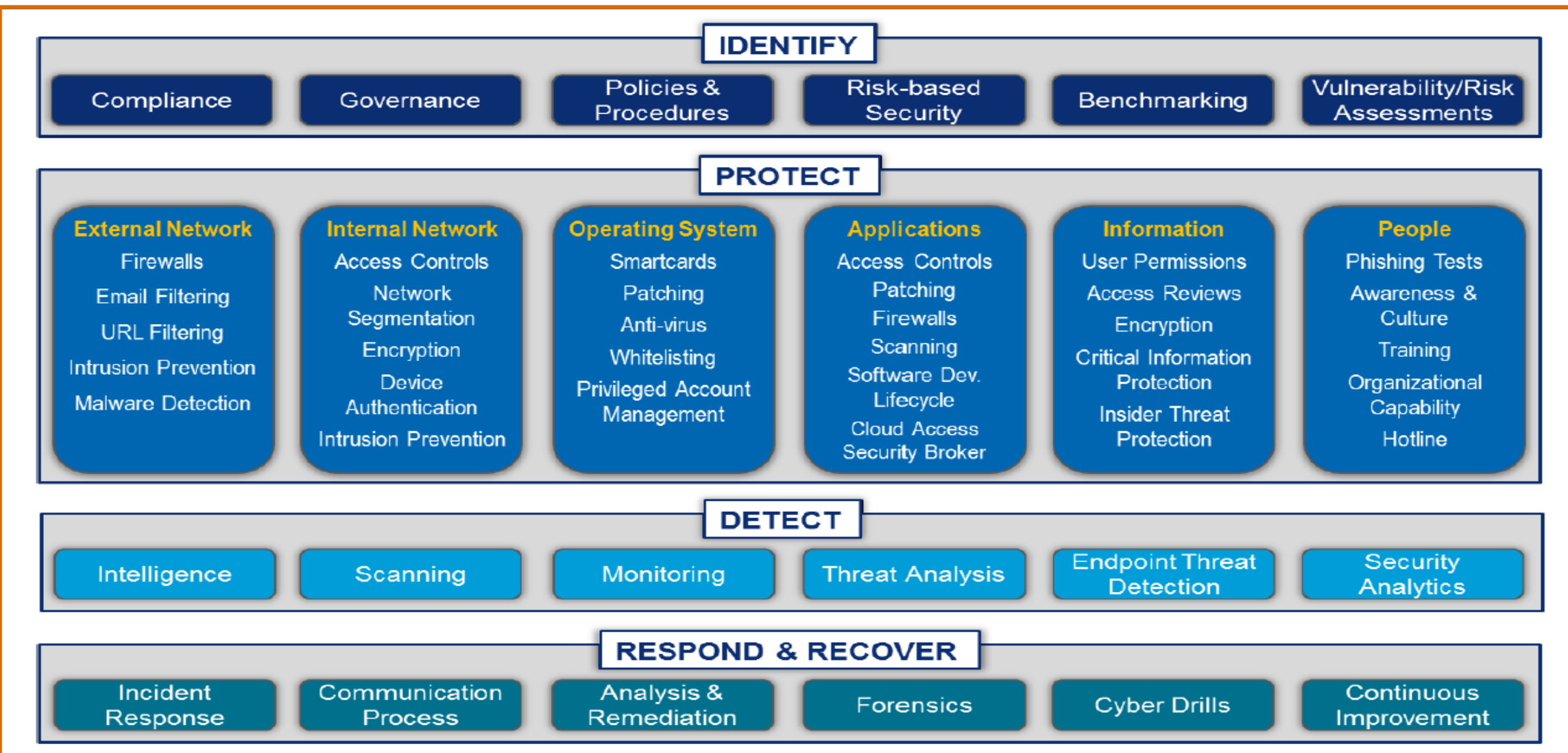
- ✓ *Implement Incident event logging management system for servers, firewalls, IDS and user's systems*
- ✓ *Log retention, preservation and permanent deletion system*

### **8 – Lessons Learned from Prior Attacks.**

- ✓ *Management should review after the fact – and organize and document the lessons learned*
- ✓ *Create Inventory of attacks experienced, the specific actions and lesson learned from prior attacks*

# *Overview of Standards*

# NIST – Cyber Security Framework

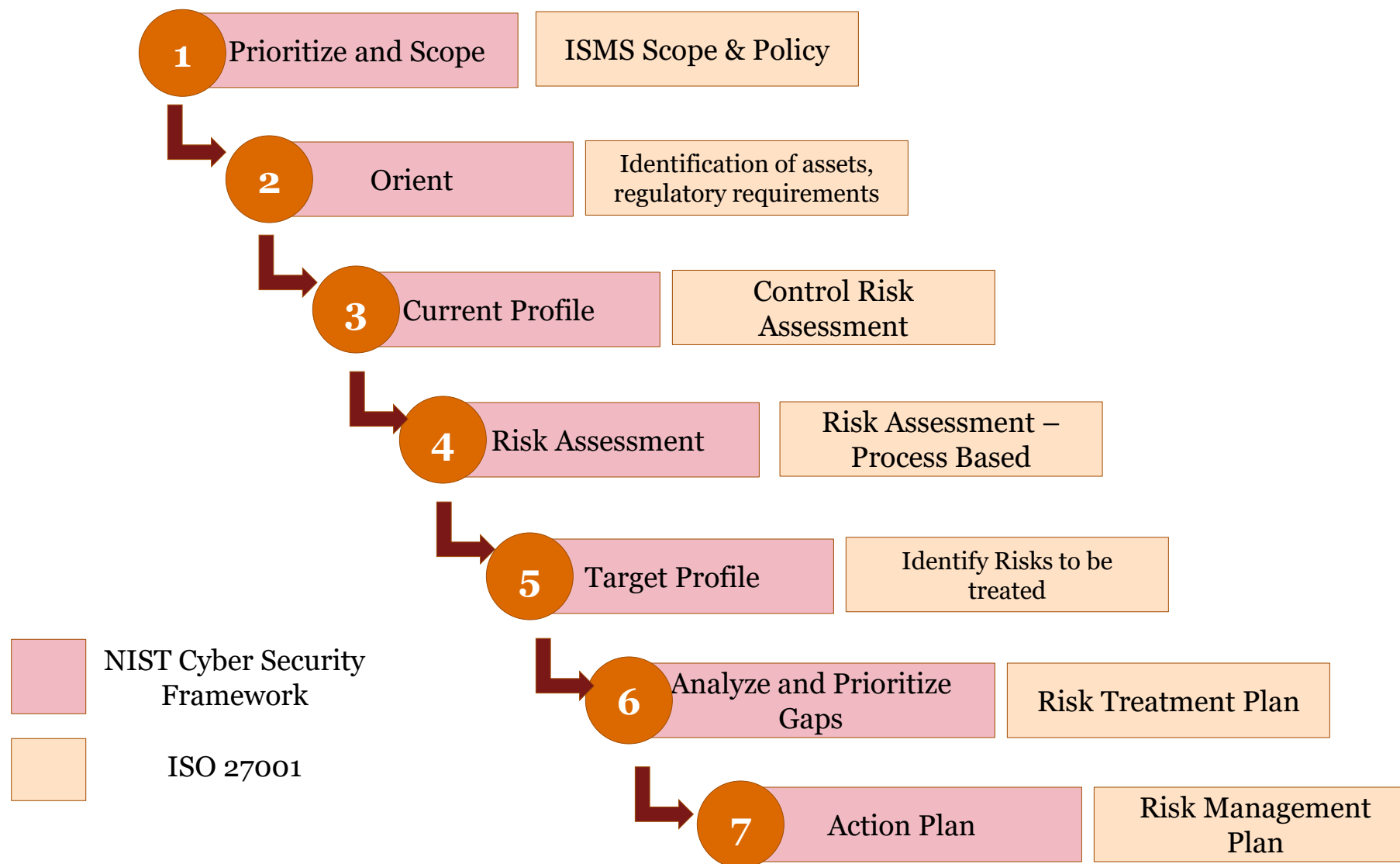


# Information Security Management System

An information security management system (ISMS) is a framework of policies, procedures, guidelines and associated resources to establish, implement, operate, monitor, review, maintain and improve information security **for all types of organizations.**



# Synergies with ISO 27001 & NIST



# ***Business Continuity and Disaster Recovery Plan***



## Major Steps in Contingency Planning

# Contingency Planning

### Business Impact Analysis

- *Identification of threats & attacks*
- *Business Unit Analysis*
- *Scenario of successful attacks*
- *Assessment of potential damage*
- *Classification of subordinate plans*

### Incident Response Planning (Focus on immediate response)

- *Incident Planning*
- *Incident Detection*
- *Incident Reaction*
- *Incident Recovery*

### Disaster Recovery Planning (Focus on restoring systems)

- *Plan for Disaster Recovery*
- *Crisis Management*
- *Recovery Operations*

### Business Continuity Planning (Focus on business availability at alternate site)

- *Establish continuity strategies*
- *Plan for continuity of operations*
- *Continuity management*



***Thank You!***