

Cyber Security

CFO Conference 2017

16 March, 2017





Agenda

- **Cyber Security Introduction**
- **Evolving Landscape, Adversaries and Impacts**
- **Key Cyber Security Risks**
- **Global Cyber Security Attacks / Breaches**
- **Information Security Regulations in Pakistan**
- **Key Takeaways / Recommendations**
- **Q&As Session**

Introduction

Saad Kaliya – Partner (Technology Consulting & Risk Assurance)

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

Saad is partner in A. F. Ferguson & Co (a member firm of the PwC network) and leads the practice of Technology Consulting and Risk Assurance. He started his carrier in assurance, however, chasing his passion, he moved to lead the technology practice of the Firm. He himself has been involved in setting up firms IT department and headed for more than 10 years where he gained an insight into working practices and security requirements for running an IT department.

Saad has been involved with the provision of diversified range of services including IT due diligence, Network penetration testing, Cyber Security and IT Risk Assessment, business continuity planning and IT disaster recovery management. He has fondness in articulating, designing and implementing business solutions.

Currently, he is also serving in IT Steering Committee of ICAP.





“

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

”

Anonymous quote on Twitter

Cyber Security

The ability to protect and defend the confidentiality, integrity and availability of information in the Cyberspace, organization and users' assets from cyber attacks.

Cyberspace is the environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it.

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 Comify.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

Hackers Steal Money from Faysal Bank Customers Once Again!

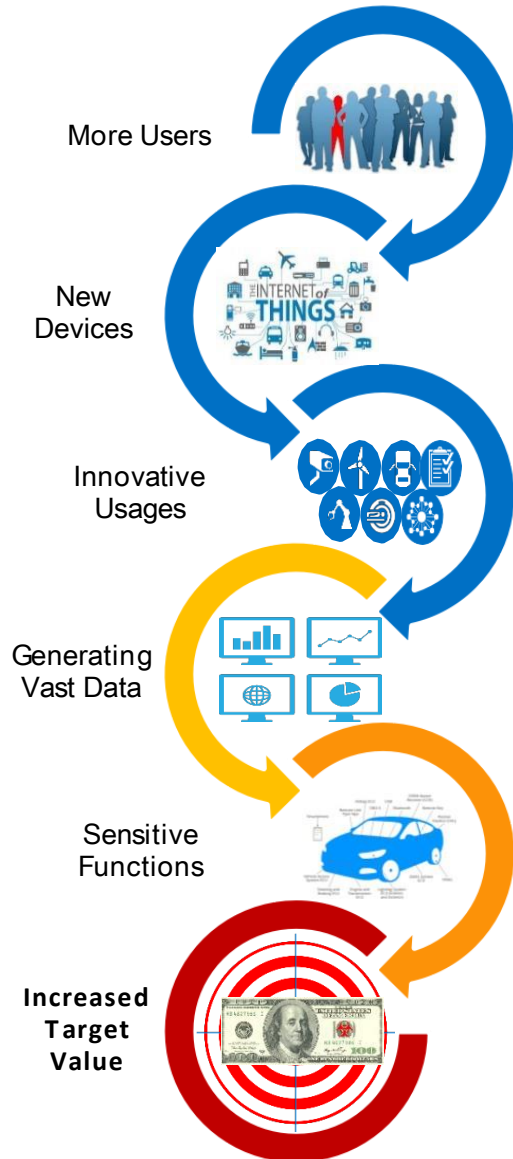
DISCLAIMER

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 Allegedly Involved in \$81 Million Bangladesh Bank Heist

Habib Bank Gets Hacked, Databases Leaked Online!

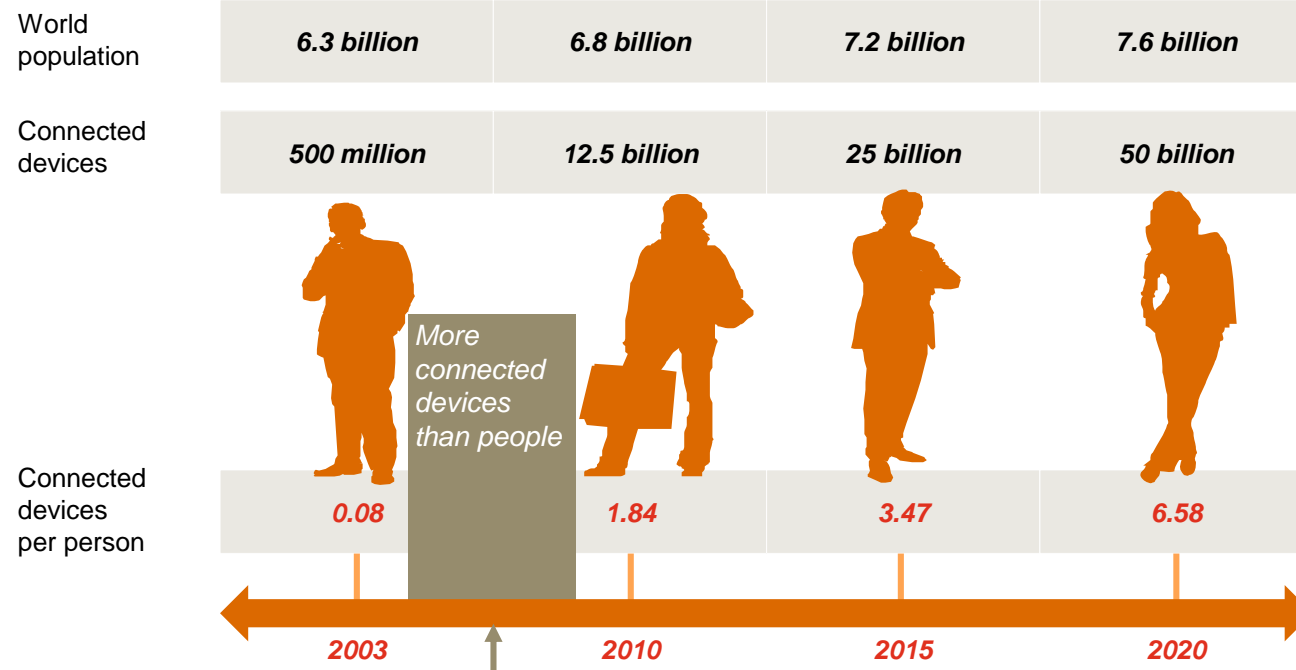
Evolving Landscape, Adversaries and Impacts



40% Increase
Data Breach disclosures from 2015 to 2016

200% increase
In cyber-crime in the last 5 years

The beginning of the 'Internet of Things'



97% of Fortune 1000 companies
Lost data or credentials 2014-2016

8 months
The average time it took from breach to detection

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

50-200 Billion Devices

Connected to the Internet

400k New Malware/Day

630 million unique samples of malware exist today

\$6 trillion

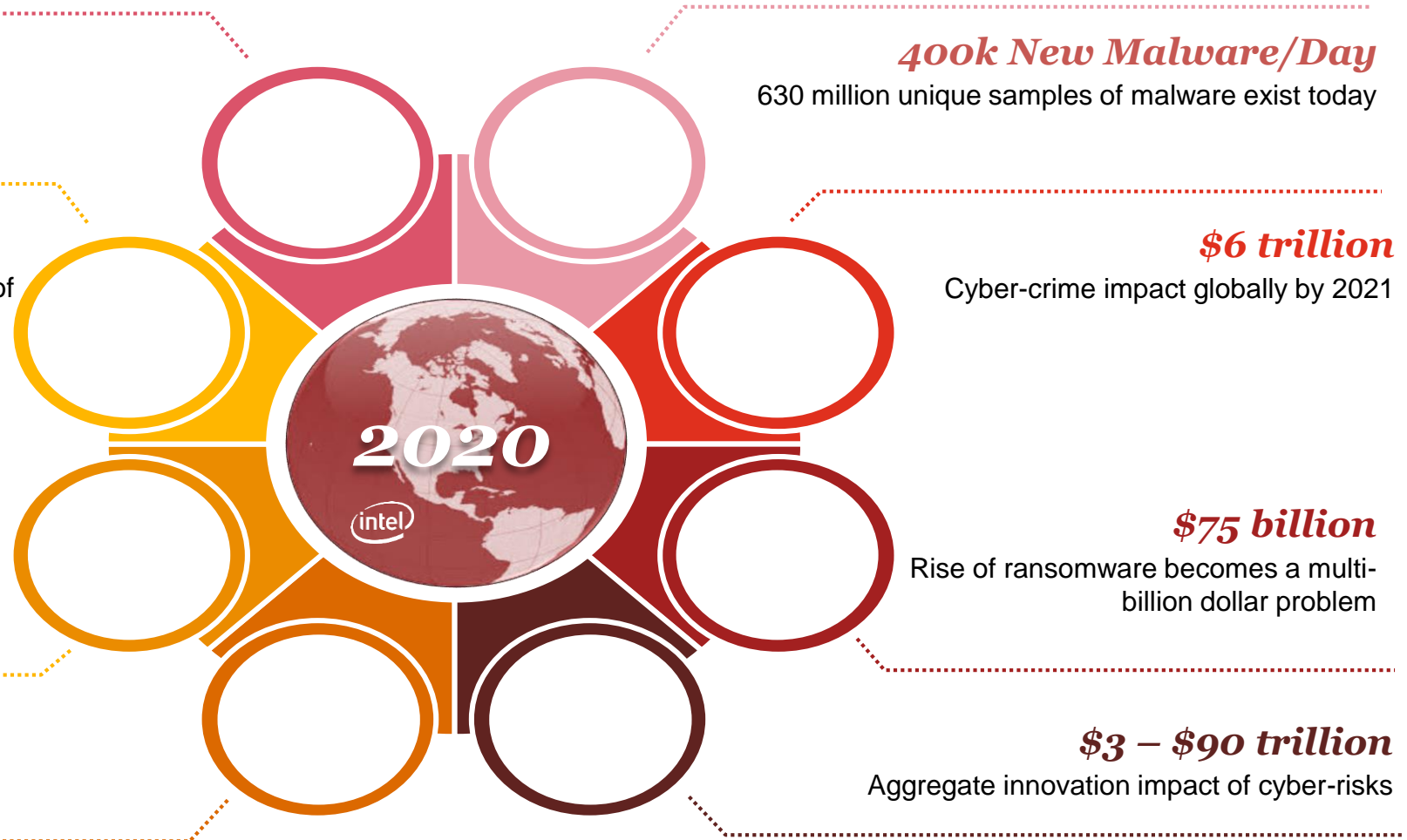
Cyber-crime impact globally by 2021

\$75 billion

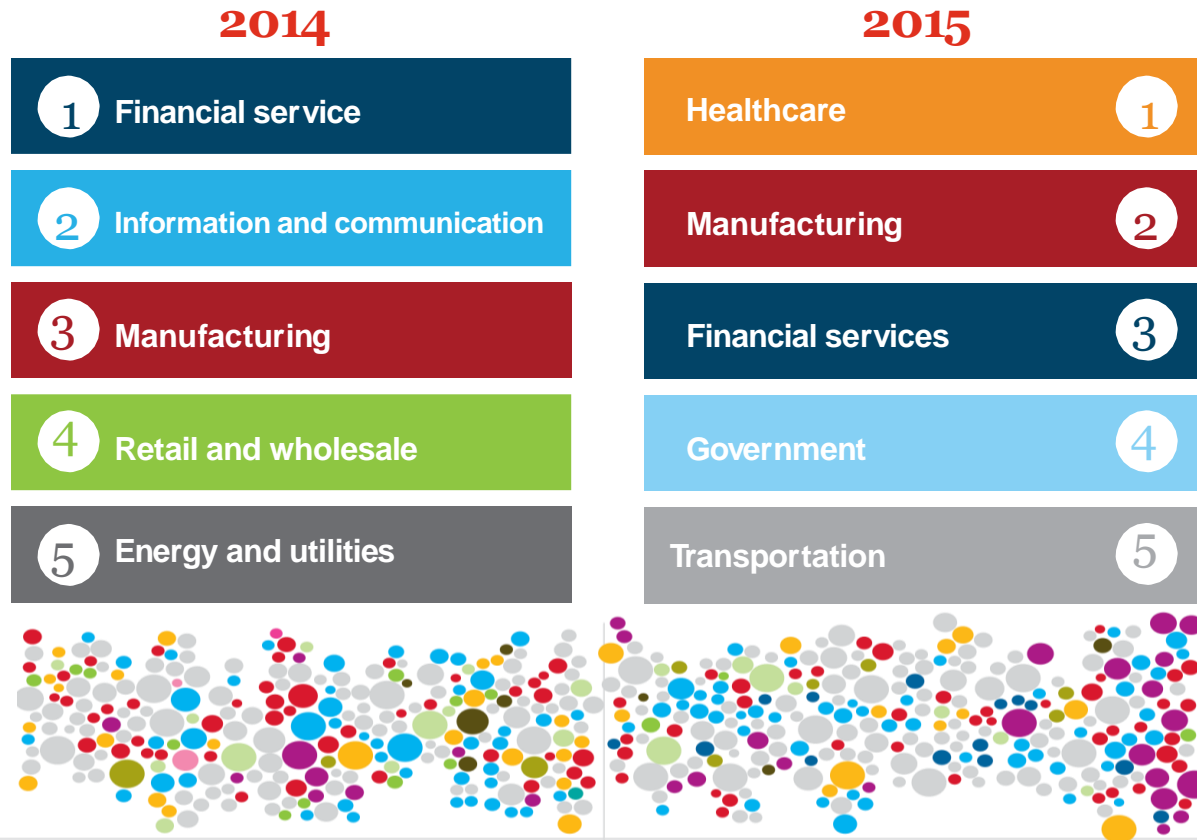
Rise of ransomware becomes a multi-billion dollar problem

\$3 – \$90 trillion

Aggregate innovation impact of cyber-risks



The 5 Most Cyber Attacked Industries



TOP 5 Cybercrimes

- Corporate account takeover
- Identity Theft
- Tax-Refund Fraud
- Theft of sensitive data
- Theft of Intellectual Property




The average cost of managing and mitigating breaches rose to \$3.1 million per incident in 2015, three times than in 2014

(2016 IBM Cyber Intelligence Index Survey)

Highlights from PwC Survey - State of Cyber Crime

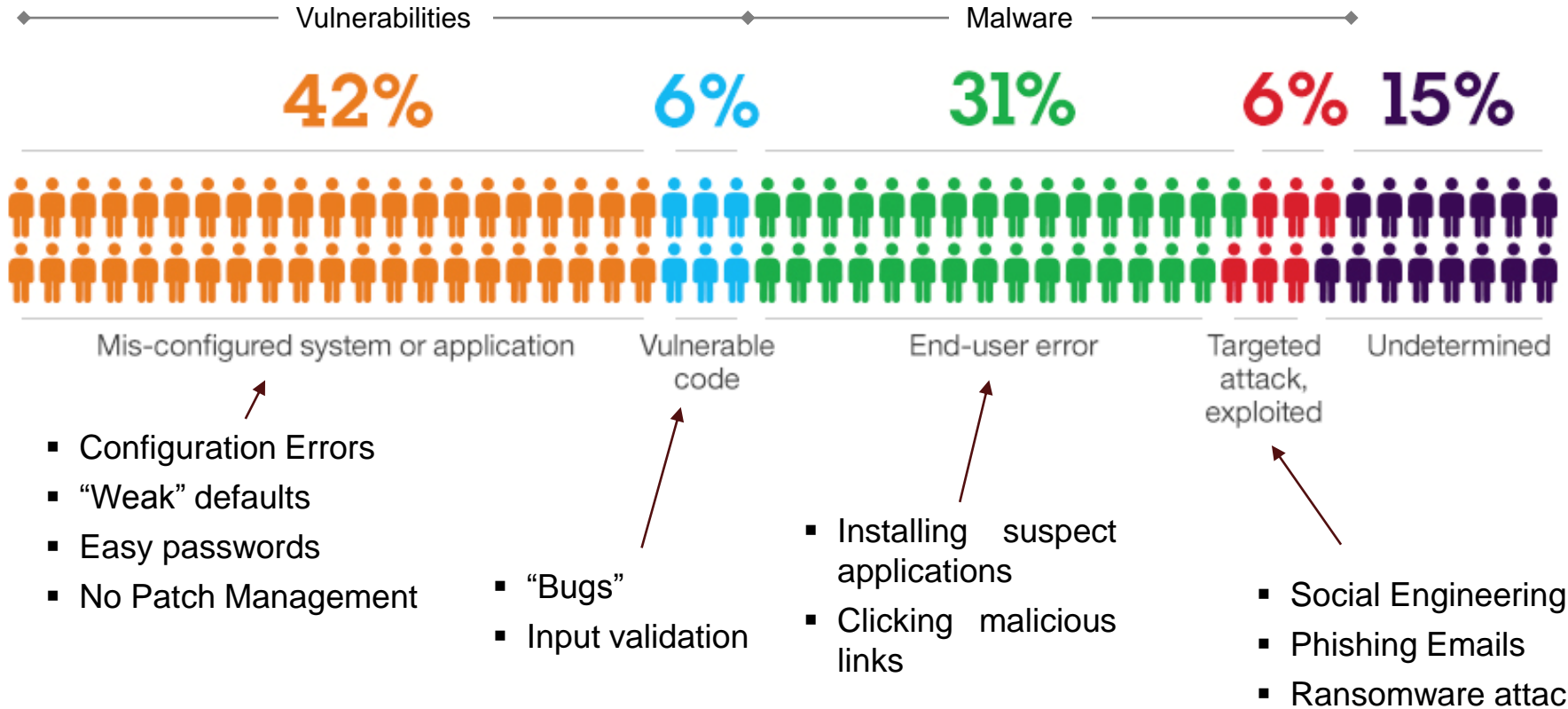
The survey identified eight common deficiencies where spending and efforts lag:

- 1. Most organizations do not take a strategic approach to cybersecurity spending**
- 2. Organizations do not assess security capabilities of third-party providers**
- 3. Supply chain risks are not understood or adequately assessed**
- 4. Cyber risks are not sufficiently assessed**
- 5. Insider threats are not sufficiently addressed**
- 6. Employee training and awareness is very effective at deterring and responding to incidents, yet it is lacking at most organizations**



Cybersecurity must be viewed as a **strategic business imperative** in order to **protect brand, competitive advantage,** and **shareholder value**

Why do Breaches Happen ?



49%  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.

Who are the hackers

Security researchers



State sponsored

Cyber criminals



Hacktivism

Key Cyber Security Terminologies

Hacking/ Ethical Hacking

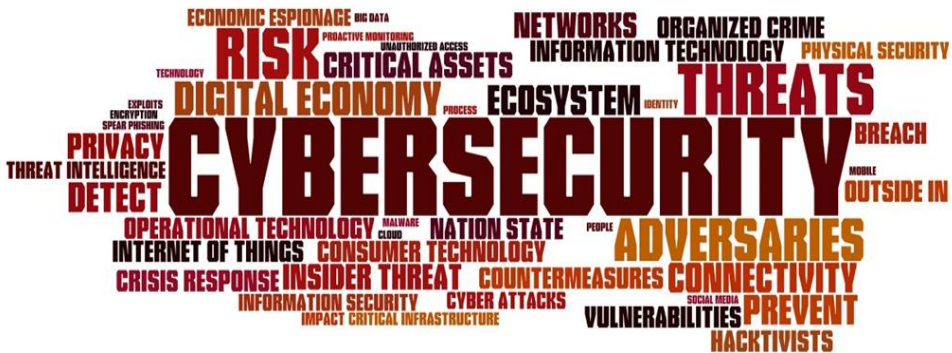
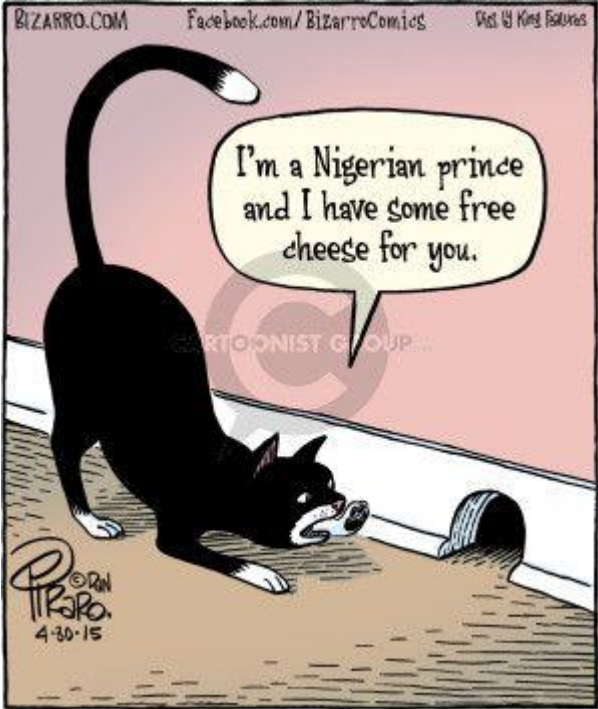
Social Engineering / Phishing

SQL Injection

Zero Day Exploits

Ransomware / Viruses

Denial of Service Attack









Global Cyber Security Breaches

There are only two types of companies: Those that have been hacked and those that will be hacked.” Robert S. Mueller, III, Director FBI

There are only two types of companies: Those that have been hacked and those that don't know they have been hacked.'

Global Cyber Security Breaches

<p>Key cyber threat scenario</p>	 <p>Banking System infiltrated by the hackers</p>	 <p>Leak of sensitive information</p>	 <p>Compromise of endpoint security through malware infection</p>
<p>Typical threat actors</p>	<p>Organized Crime, Hackers, hackers</p>	<p>Hackers, hacktivists, chancers</p>	<p>Organised criminals, nation states</p>
<p>Primary Motivations</p>	<p>Financial Gain</p>	<p>Financial Gain, Identity Theft</p>	<p>Financial gain, espionage</p>
<p>Recent example</p>	 <p>Bangladesh Central Bank</p> <p>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 a bank in the Philippines</p>	 <p>In 2016, Yahoo announced that hackers have stolen sensitive user details resulting decline in stock price.</p>	 <p>Sony was the victim a targeted email phishing campaign resulting in the compromise of sensitive information and significant reputational damage</p>

Global Cyber Security Breaches

Key cyber threat scenario



Infiltrate Bank's system using malware, which lurked in network for months



Hack of logical security



Direct Compromise of Internet Accessible System

Typical threat actors

Organised criminals, nation states

Organised criminals

Hackers, hacktivists, chancers

Primary Motivations

Financial gain, espionage

Financial Gain, Identity Theft

Fun, Identity Theft

Recent example



Hacker breached bank demanding ransom of \$3 million ransom to step tweeting data mostly corporate accounts, hacker dumps tens of thousands of customers' transactions history online.



Nearly 10,000 frequent flyer accounts were possibly compromised when criminals used stolen usernames and passwords to access the accounts, book trips and redeem flight upgrades.



38 million users signed up to the dating service had their personal details leaked online by moral hackers looking to shut down the site

What's the impact of a cyber attack?

Consider the impacts of fraud and espionage

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

Information Security Regulations / Circulars in Pakistan

*Digital
revolution*



*Growing
cyber risk*



*More
regulation*

State Bank of Pakistan

- ✓ Guidelines on Business Continuity Planning
- ✓ Information Technology Security
- ✓ Security of Internet Banking
- ✓ Payment Card Security
- ✓ Prevention against Cyber Attack

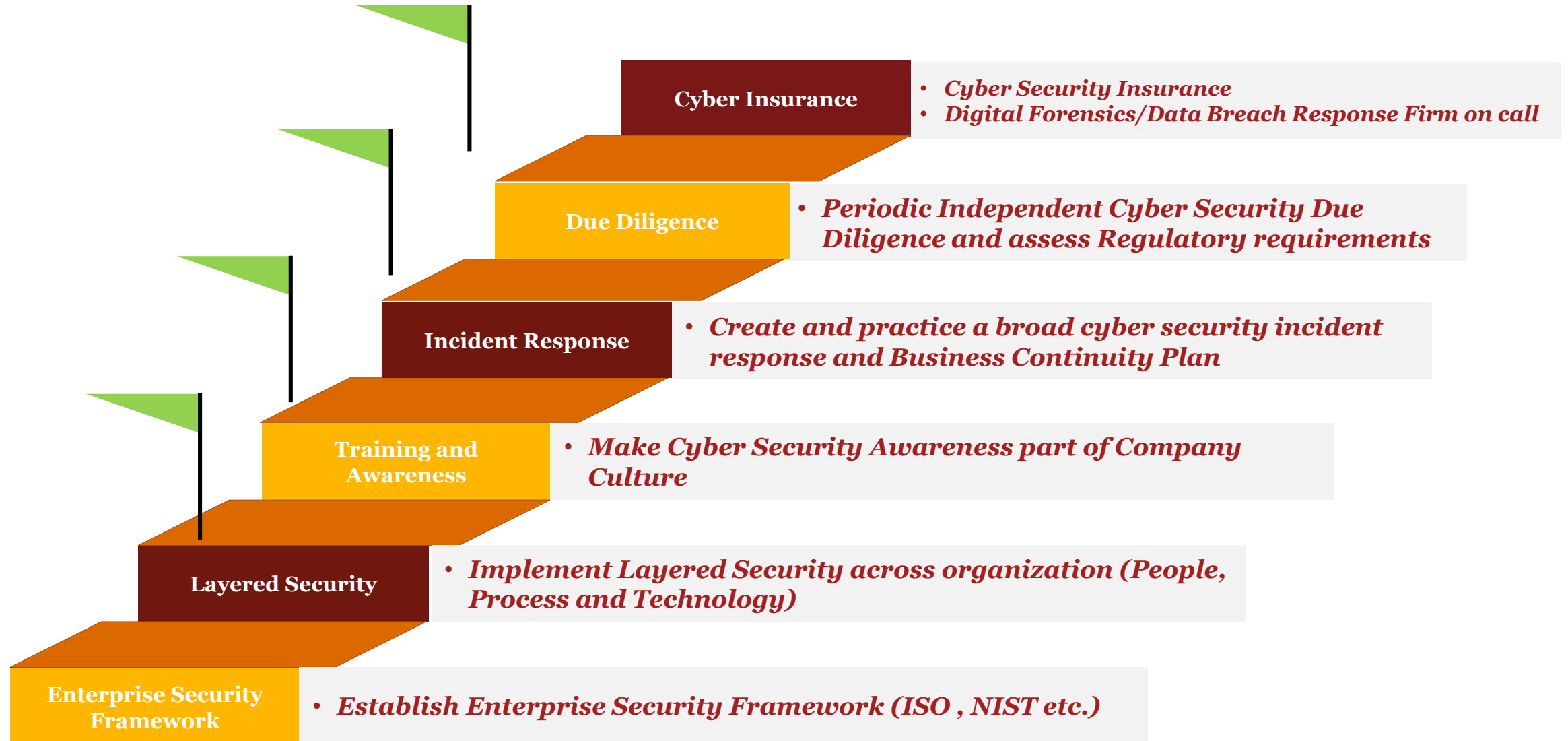
Prevention of Electronic Crime Bill -2016

- ✓ 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

Key Questions of Executive Round Table Session



Key Takeaways from Round Table Session



In the end....

Cyber criminals only need to get it right once we need to get it right always.