CYBER STRATEGY
A practitioners perspective

Cyber Risk Management & Oversight through effective IT Governance

Cyber Risk Conference
26 – 27 July 2018

RADHEY SHYAM

COO, APAC IT
AIG APAC Holdings Pte. Ltd.
Radhey.shyam@aig.com
+65 98340342

Agenda

- ✓ CYBER ECO-SYSTEM
  - Quick review of the digital / cyber revolution and information opportunities.
- ✓ RISK
  - Evidence for informed information risk approach as alternative to IT/ Cyber Security based approach.
- ✓ RESILIENCE
  - Review of approaches to manage CYBER induced risk.

Cyber Strategy

- Cyber Strategy refers to the prevention & management of RISK induced by adoption of Information Technology components / integration to Digital ecosystem.
- Key parts of the strategy:
  - ✓ **Prevention** – Deter attacks to prevent loss.
  - ✓ **Prediction** – Ability to predict attacks.
  - ✓ **Detection** – identifying attacks not preventable and triggering appropriate response.
  - ✓ **Response** – Incident management, to prevent loss and return to normalcy.

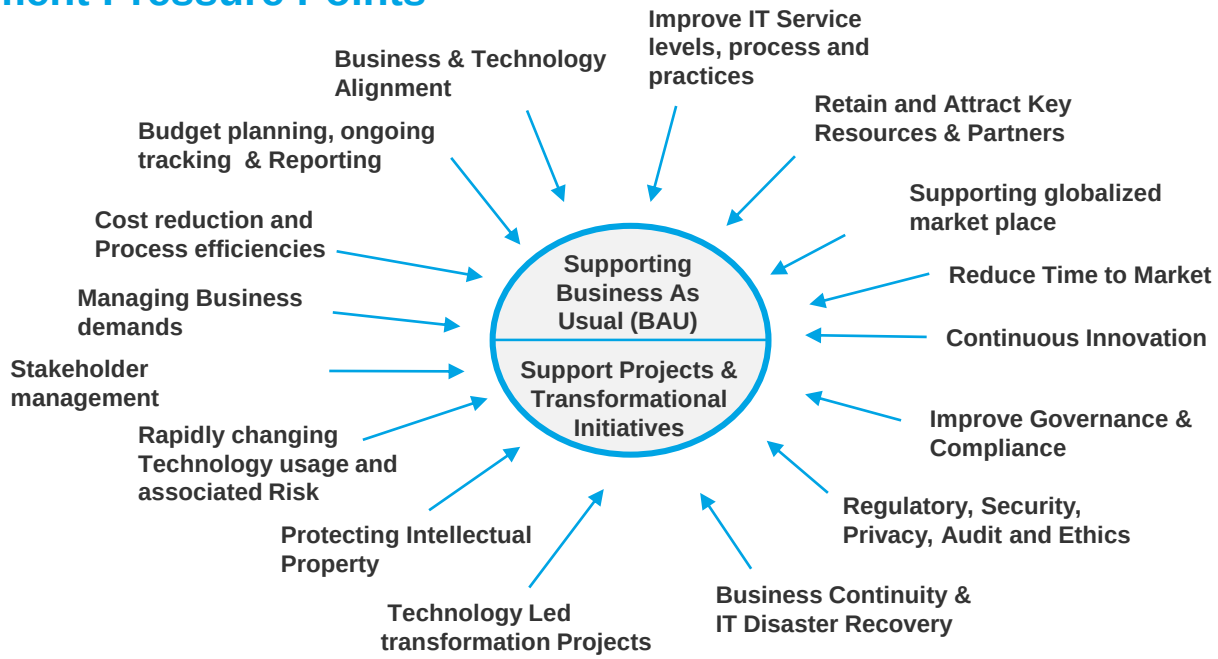
Digital Ecosystem

An overview

Fundamental Questions for Corporate IT departments

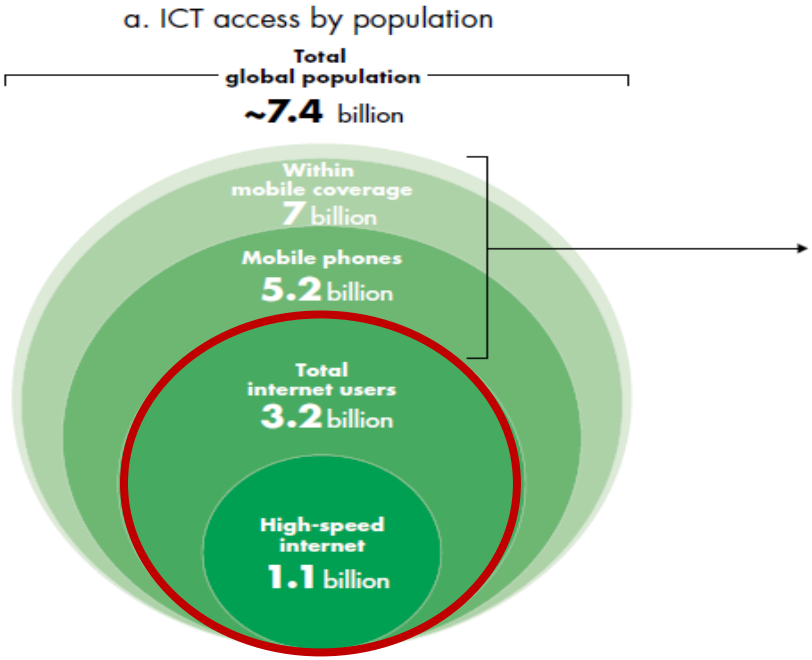
- Are we maximizing the value of IT Investments?
- Is it at affordable cost?
- Are we complementing the business?
- What are the RISK's and what level of RISK is acceptable?

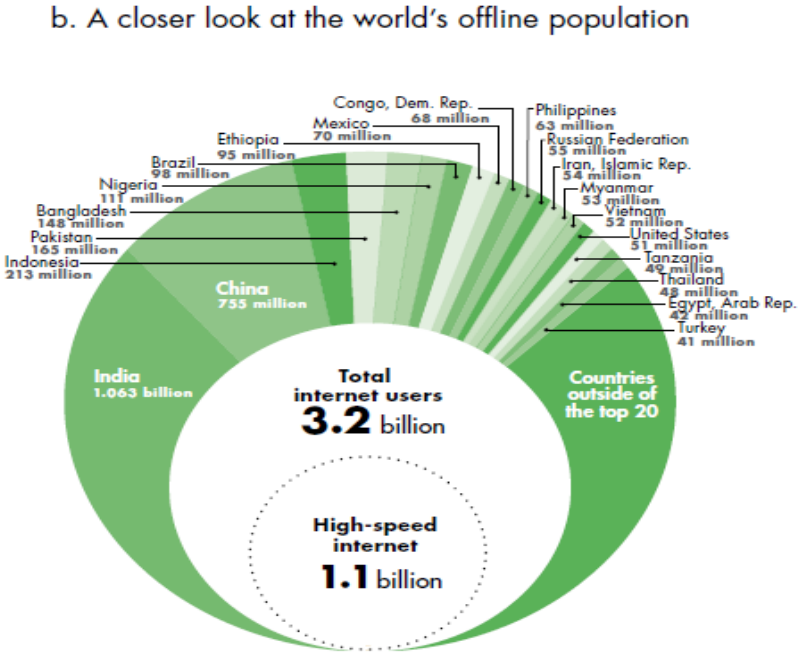
IT Management Pressure Points

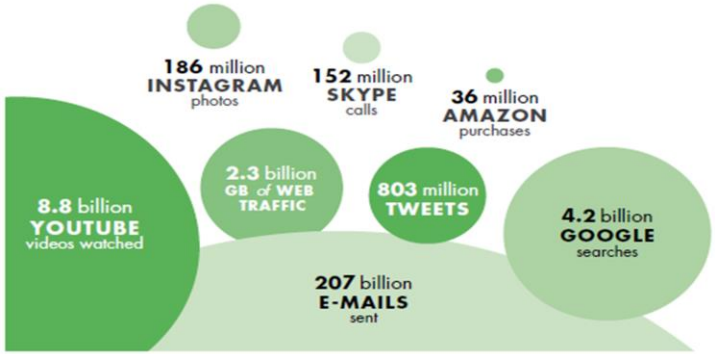


Digital Ecosystem

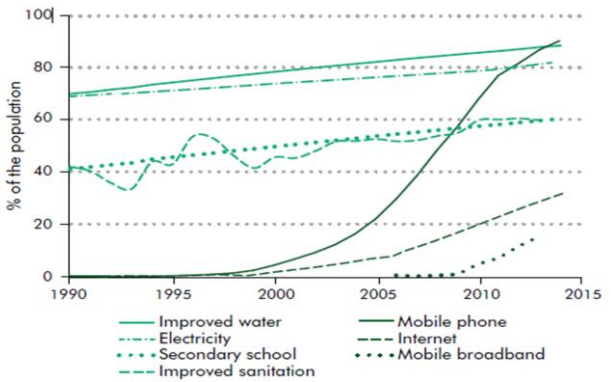
An overview







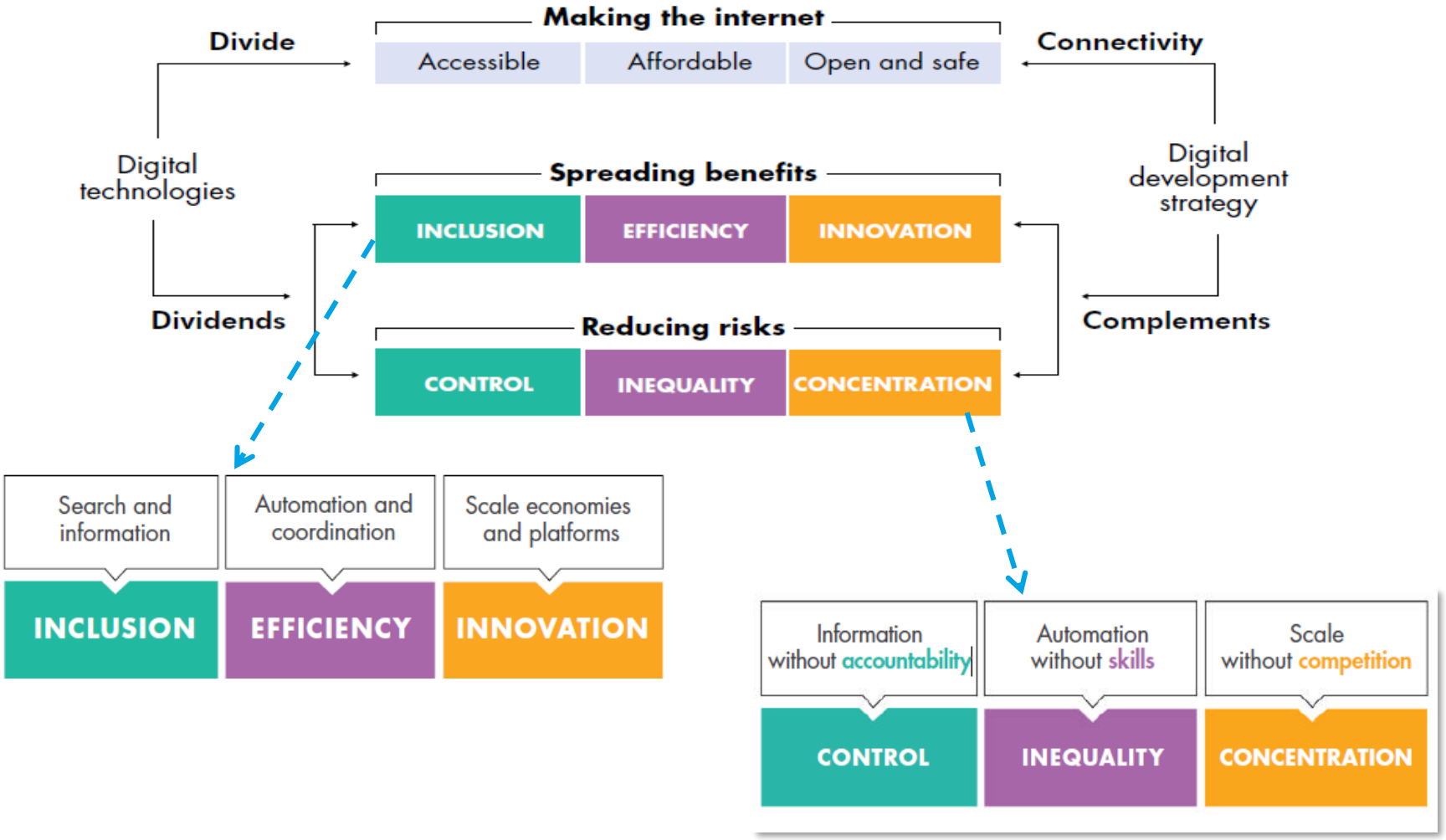
A day in the life of Internet…



Source: WDR 2016 team, World Bank. – Digital Dividends

Digital Ecosystem

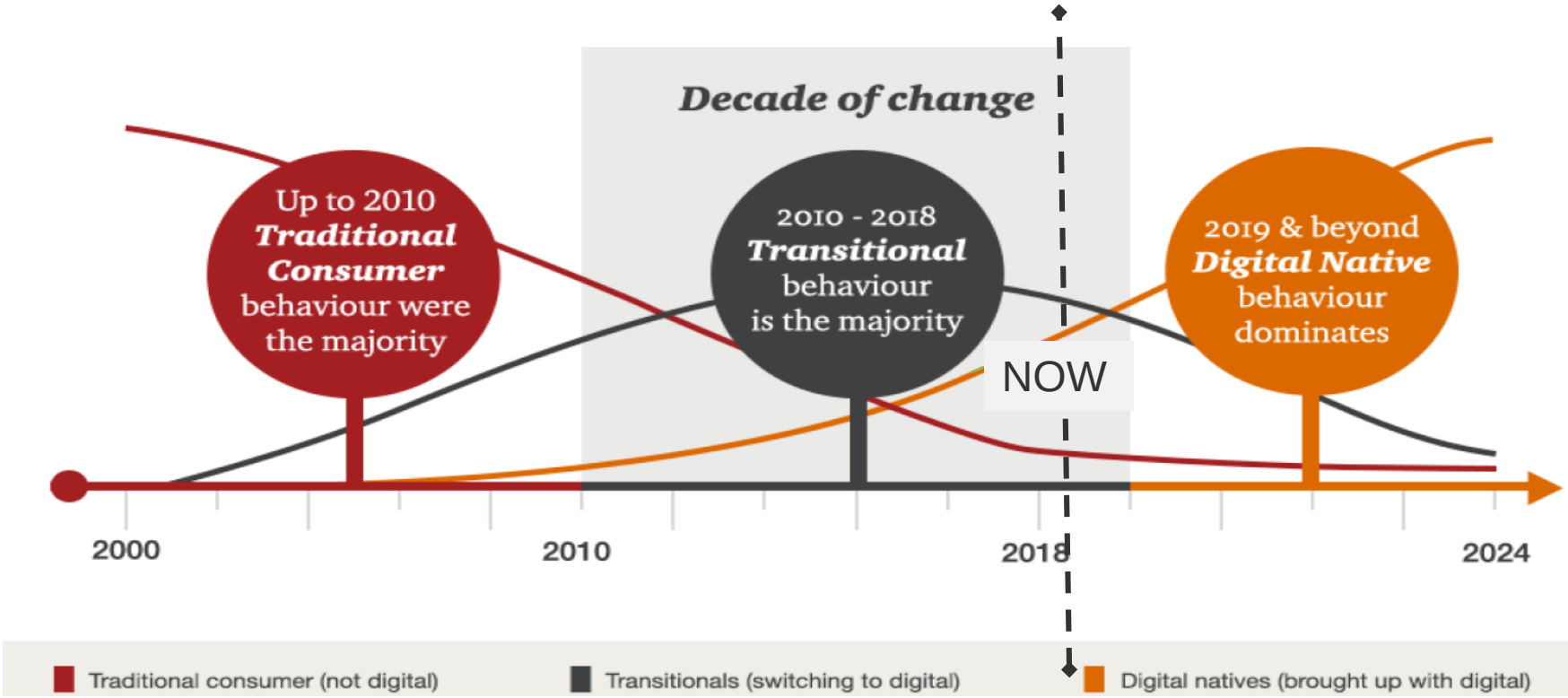
Building blocks for Digital Economy…



Source: WDR 2016 team, World Bank. – Digital Dividends

Digital Ecosystem

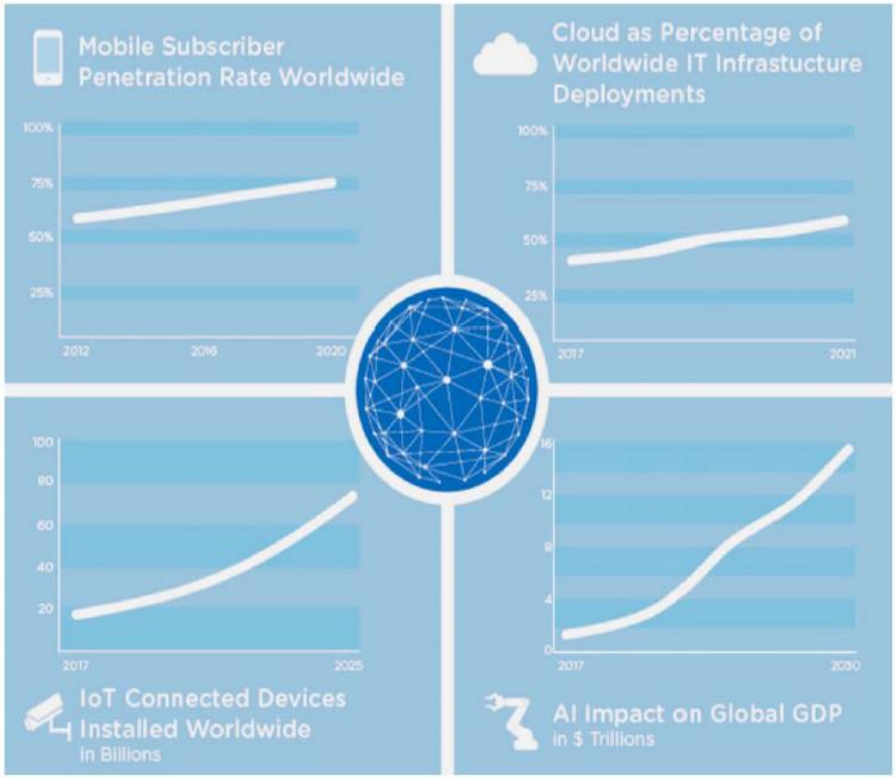
Digital Economy, a new industrial evolution?



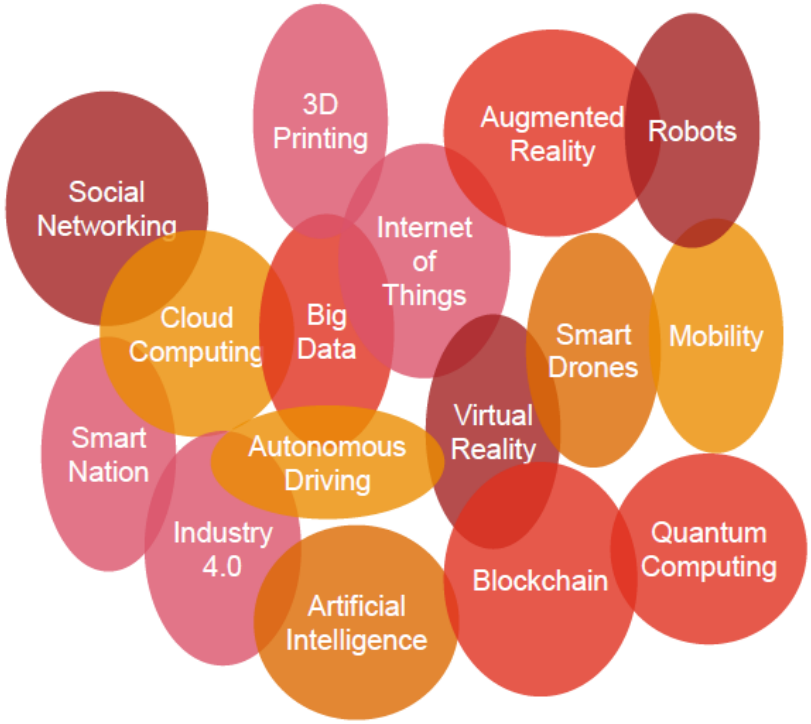
Source: *PWC – Trust in Digital Age*

Digital Ecosystem

Tech catalysts leading the evolution…



The global reach of these four tech superpowers is speeding up
Image: Pat Gelsing

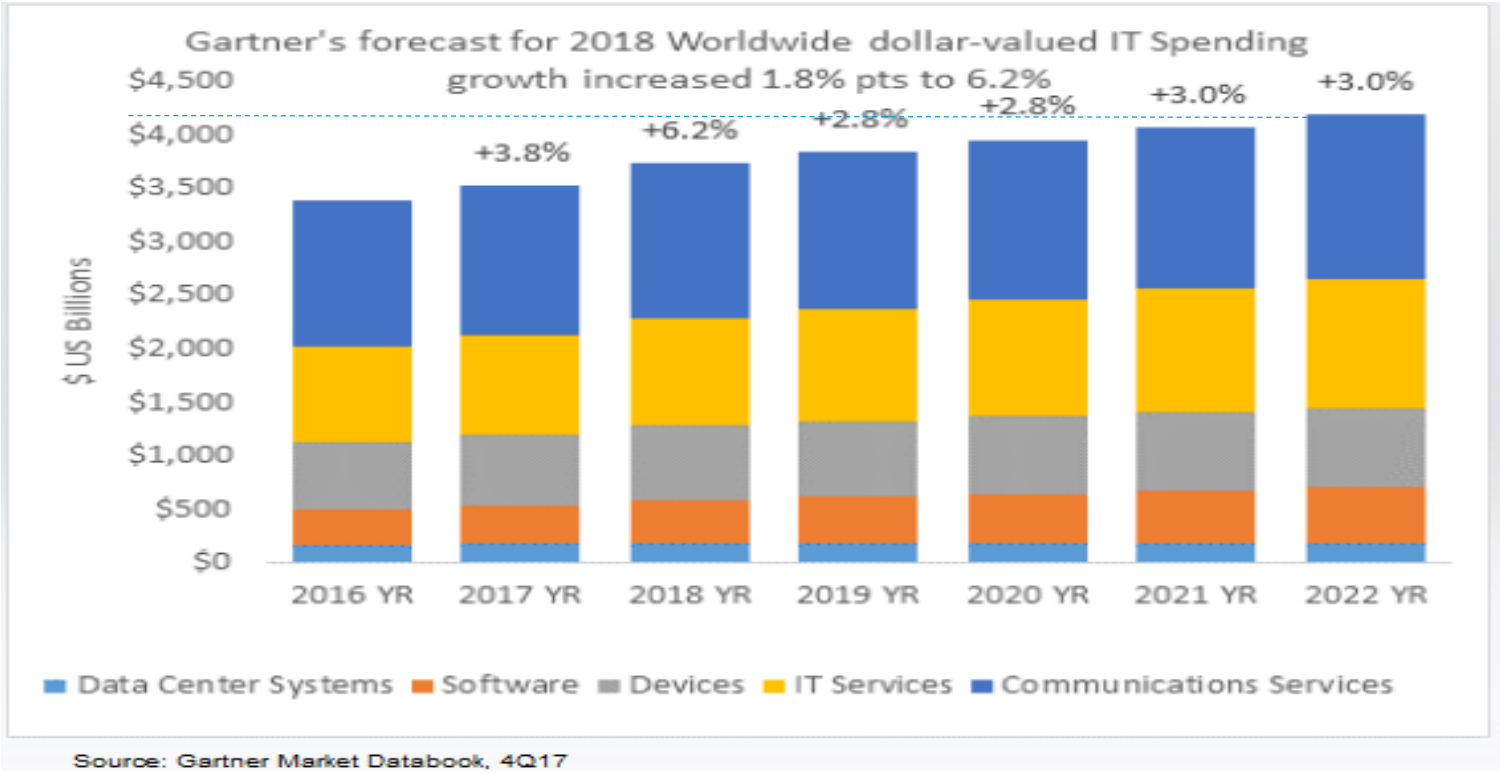


- ✓ World Economic Forum has named the above Four Technologies as ‘Super-powers’ that’s fronting digital transformation.
- ✓ Other technology enablers…

Source (left): World Economic Forum - Four new ‘superpowers’ you should know about
Source (right): PWC – Trust in Digital Age

Digital Ecosystem

Spending Projections…

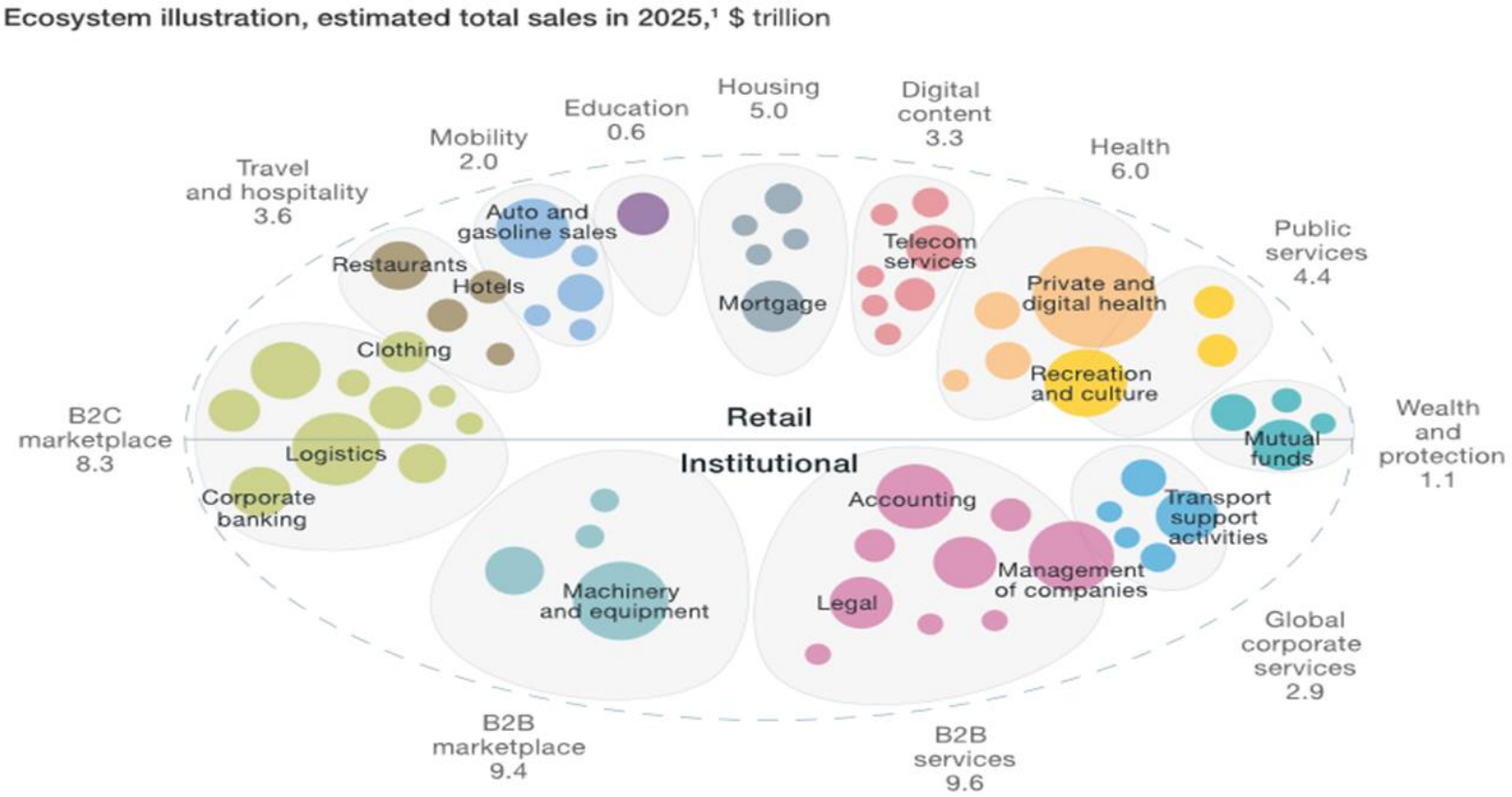


Worldwide IT spending is projected to total $3.7 trillion in 2018, an increase of 4.3% from 2017 estimated spending of $3.5 trillion, according to the latest forecast by Gartner, Inc.

Source: https://gartner.gcs-web.com/news-releases/news-release-details/gartner-says-global-it-spending-reach-37-trillion-2018

Digital Ecosystem

The World Bank projects the combined revenue of global businesses will be more than $190 trillion within a decade.

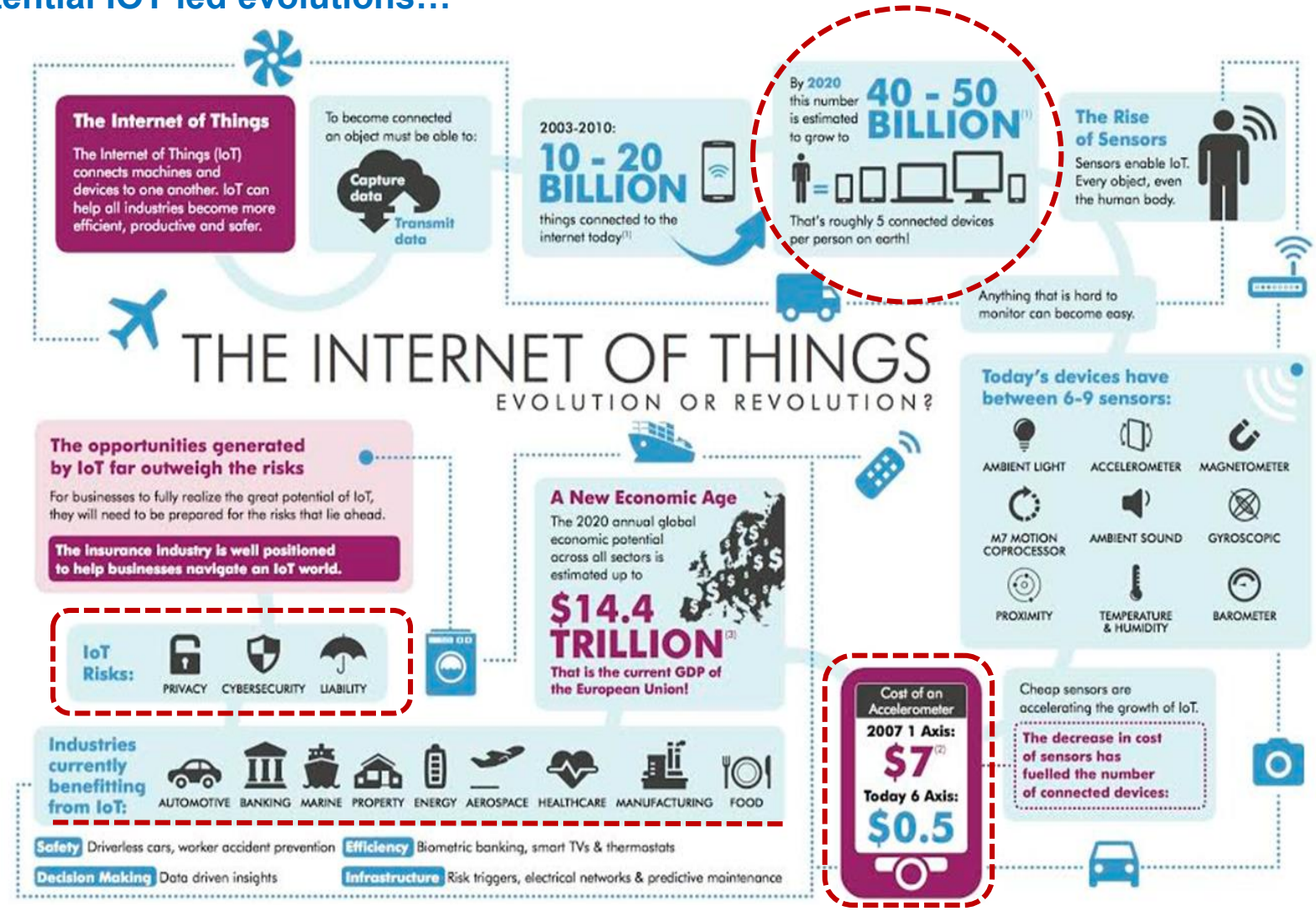


New business Eco-systems are likely to emerge & replace the traditional business models by 2025.

Source: https://www.mckinsey.com/business-functions/mckinsey-analytics/our-insights/competing-in-a-world-of-sectors-without-borders

Digital Ecosystem

Potential IOT led evolutions…



Source: https://www.aig.com/innovative-tech

Digital Ecosystem

Evolving Risk Conditions...

- **Physical Attack** – Attack on critical infrastructure has potential to disrupt critical services.
- **Cyber Crime is now commoditized** – Non-technical person can now subscribe into Cyber Crime. E.g., Ransomware as service and botnet as services are examples.
- **Cyber crime gets smatter** – Easy availability computing (IOT, Cloud, etc.) resources & intelligent (AI) software components is likely to increase automated, intelligent & targeted attacks.
- **Data & National security** – More nations are viewing data in line with national security and restricting cross boarding data hosting & sharing.
- **Political Threats** – Cyber technology/warfare is considered the new frontier. Has potential to disrupt economies & critical infrastructure.

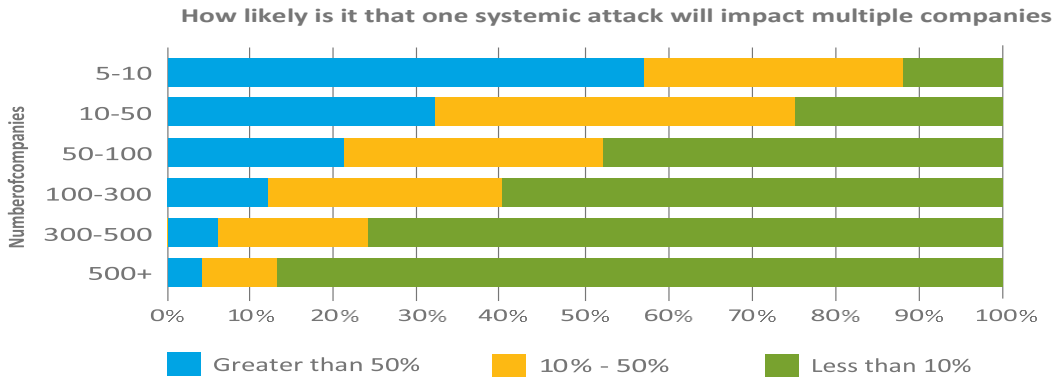
Source: http://dilbert.com/

Digital Ecosystem

Evolving Risk Conditions...

In December 2016, AIG surveyed cyber security and risk experts to gain a deeper understanding of their views of the likelihood and impact of a systemic cyber-attack.

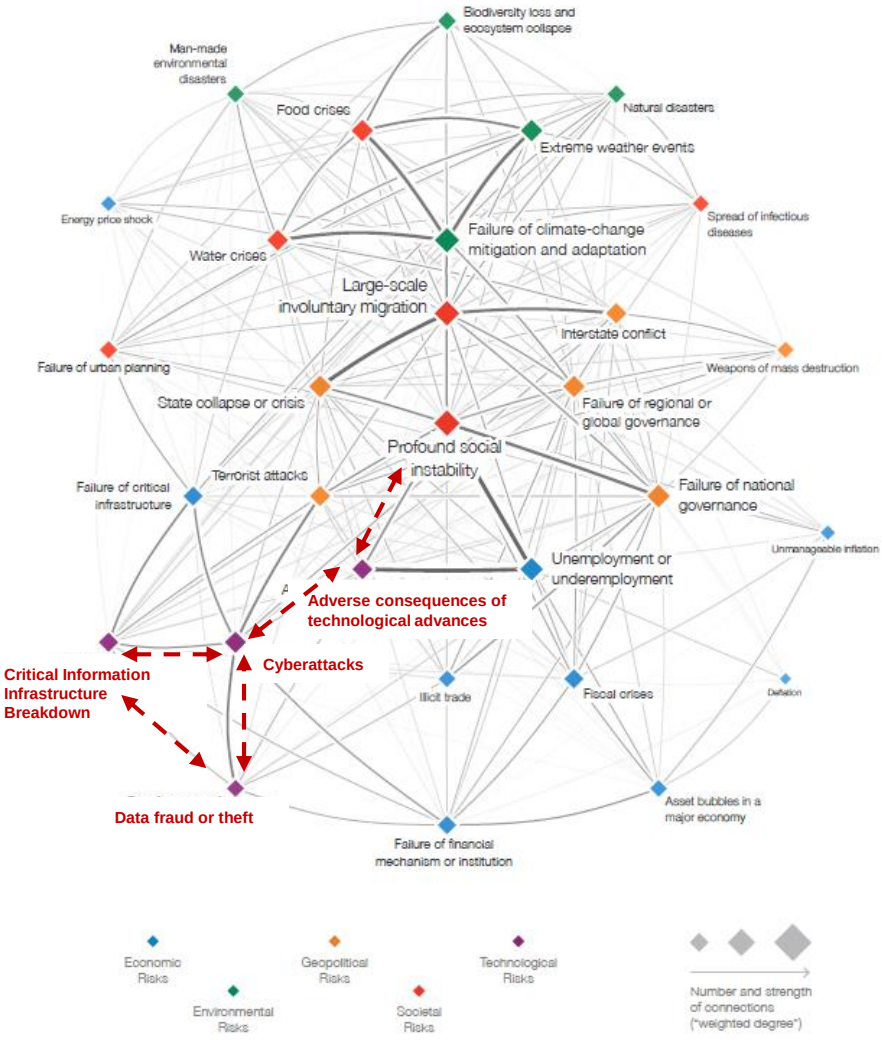
- More than 90% of respondents believe that cyber risk is **systemic**, i.e., capable of impacting many companies at the same time.



Global cyber risks are expanding as the use of connected devices soars. The number of connected devices worldwide is expected to reach 46 billion by 2021, a 200% increase from 2016.[xiii] "The unceasing proliferation of technology, the increase in network speed, and an explosion in data…are multiplying the potential attack surface for malicious actors," says Mark Camillo, AIG's Head of Cyber, EMEA. "The growth of the internet of things (IoT) has introduced vulnerabilities, as not all connected devices are currently designed with security in mind."[xiv]

Digital Ecosystem

Cyber Risk and its integration with Global Risk…



Top 10 risks in terms of
Likelihood

1. Extreme weather events
2. Natural disasters
3. Cyberattacks
4. Data fraud or theft
5. Failure of climate-change mitigation and adaptation
6. Large-scale involuntary migration
7. Man-made environmental disasters
8. Terrorist attacks
9. Illicit trade
10. Asset bubbles in a major economy

Top 10 risks in terms of
Impact

1. Weapons of mass destruction
2. Extreme weather events
3. Natural disasters
4. Failure of climate-change mitigation and adaptation
5. Water crises
6. Cyberattacks
7. Food crises
8. Biodiversity loss and ecosystem collapse
9. Large-scale involuntary migration
10. Spread of infectious diseases

AIG

Source: World Economic Forum Global Risks Perception Survey 2017–2018

Digital Ecosystem

Security Incidents...

In late 2016 and early 2017, hackers launched an **extortion campaign:**

- Security researchers suggest that between 50,000 and 100,000 MongoDB databases were exposed globally.

- Ransomware – hackers were able to lock-up data and critical computing resources.

2016 & 2017	UniCredit, Italy's largest bank lost 400,000 client details to hackers.
Q4 2016	Hackers carried out UK's largest cyber robbery of ~2.5M GBP from Tesco bank.
2016	Hackers stole SWIFT code and stole ~81M USD from Bangladesh's central bank's account.
April 2014 to June 2017	Reserve Bank of India indicate that Indian banks lost ~85K INR per hour, facing ~40 attacks per day.

And many more attacks …

Source: https://www.aig.com/knowledge-and-insights/k-and-i-article-state-of-cybersecurity-industries-services-individuals

Digital Ecosystem

Security Incidents…

CNN tech BUSINESS CULTURE GADGETS FUTURE STARTUPS CNNM

Massive data theft hits 40% of South Koreans

by Sophia Yan and K.J. Kwon @CNNTech

January 21, 2014: 2:49 AM ET

The personal data of 20 million South Koreans -- or 40% of the country's population -- has been stolen, sparking outrage as worried consumers scramble to replace compromised credit cards.

Customer details appear to have been swiped by a worker at the Korea Credit Bureau, a company that offers risk management and fraud detection services.

The worker, who had access to various databases at the firm, is alleged to have secretly copied data onto an external drive over the course of a year and a half.

Clients of three Korean companies -- KB Kookmin Bank, Lotte Card and Nonghyup Bank -- were hardest hit by the data theft. Crucial personal data like identification numbers, addresses and credit card numbers were all stolen.

VIDEOS EXECUTIVE GUIDES SECURITY CLOUD INNOVATION CXO HARDWARE MORE

MUST READ WHY DID MICROSOFT BUILD THE SURFACE GO?

StanChart client data stolen in Singapore via Fuji Xerox server

Monthly statements belonging to 647 private banking clients were stolen via the bank's outsourced printing services provider. The theft was discovered after the files were found on a laptop recently seized from alleged hacker "The Messiah".

By Ryan Huang | December 6, 2013 -- 03:29 GMT (11:29 GMT+08:00) | Topic: Security

DBS. Living, Breathing Asia DBS

Ref: 21/2010

DBS and IBM detail findings of 5 July outcome

***

SINGAPORE,04 August 2010 - **DBS AND IBM DETAIL FINDINGS OF 5 JULY OUTAGE**

***

Wide range of actions underway to prevent recurrence

Singapore, 4 August 2010 – DBS and IBM today announced that the portion of the investigation into the DBS systems outage on 5 July 2010 related to determining the cause of the incident has been concluded. DBS and IBM jointly provided a detailed account of events which preceded the outage, and consequent recovery activities and actions.

Singapore

Personal data of 5,400 AXA Singapore customers exposed in cyberattack

CHANNEL NEWSASIA Singapore Edition My News Feed Bookmarks Watch TV

Singapore Asia World CNA Insider Business Sport Lifestyle Technology Health Commentary Podcasts ASEAN Video on Demand

Singapore

24 Jul 2018 06:07PM
(Updated: 25 Jul 2018 12:11AM)

SingHealth cyberattack: MAS orders financial institutions to tighten customer verification

AIG

Source (left):
https://money.cnn.com/2014/01/21/technology/korea-data-hack/index.html
https://www.channelnewsasia.com/news/singapore/personal-data-of-5-400-axa-singapore-customers-exposed-in-9194674
Source (right):
https://www.zdnet.com/article/stanchart-client-data-stolen-in-singapore-via-fuji-xerox-server/
https://www.dbs.com/newsroom/print-news.page?newsId=i0bk3qxp&locale=en
https://www.channelnewsasia.com/news/singapore/singhealth-cyberattack-mas-financial-institutions-verification-10558690

Digital Ecosystem

Key Regulatory Changes in reaction to the Risk…

- ✓ United States Cybersecurity Law
- • Computer Fraud and Abuse Act
- • Electronic Communications Privacy Act
- ✓ Critical Infrastructure and Information Sharing
- • February 2013: Executive Order 13636
- • February 2014: NIST releases Cybersecurity Framework and CI Cyber Community
- • Cybersecurity Act of 2015
- ✓ Protecting Personal Information
- • Massachusetts data security law; Gramm-Leach-Bliley Act, HIPAA, Communications Act
- ✓ Canada Cybersecurity Law
- • Criminal Code; Personal Information Protection & Electronic Documents Act;
- ✓ United Kingdom Cybersecurity Law
- • Computer Misuse Act of 1990 (Amended in 2006)
- ✓ EU – Cybersecurity Framework
- • EU Network and Information Security (NIS) Directive
- • General Data Protection Regulation
- ✓ French Cybersecurity Law
- ✓ German Cybersecurity Law
- • IT Security Act (ITSG) (2015)
- • Télécommunications Act (2014)
- ✓ Estonian Cybersecurity Law
- ✓ Chinese Cybersecurity Law
- ✓ Japanese Cybersecurity Law
- ✓ South Korean Cybersecurity Law
- • Personal Information Protection Act (PIPA).
- ✓ Indian Cybersecurity Law
- ✓ **Singapore Cybersecurity Law**
- • **Tech Risk Mgt, Consumer Protection Act, PDPA, IT TRM, Cybersecurity Bill…**
- ✓ Australia Cybersecurity Law
- ✓ UAE Cybersecurity Law
- • Otoritas Jasa Keuangan [OJK] of Indonesia

Cybersecurity and the Board: 8 Issues Keeping Directors up at Night

By Paula Loop, Leader, PwC's Governance Insights Center

Posted on October 11, 2016

Cyber threats continue to be a major concern for companies and boards today. Companies saw 38% more detected security incidents in 2015, and the average total financial loss because of those incidents was $2.5 million. It's no surprise, then, that 88% of US CEOs are worried that cyber threats could impact growth prospects.[1] How can companies and boards stay on top of this complex and dynamic situation?

KEY FOCUS

- ✓ Personal Information Protection
- ✓ Securing Critical Infrastructure, including Network operations
- ✓ Data sovereignty / Geographical restrictions
- ✓ Minimum / Acceptable technology standards
- ✓ Incident reporting and Management
- ✓ Penalties

Source: (bottom left) https://www.opengovasia.com/sector/government
Source: (top left) https://sponsoredcontent.wsj.com/pwc/broader-perspectives/cybersecurity-and-the-board-8-issues-keeping-directors-up-at-night/
Source: (top) https://www.rsaconference.com/writable/presentations/file_upload/law-w04-global_cybersecurity_laws_regulations_and_liability.pdf

Cyber Resilience

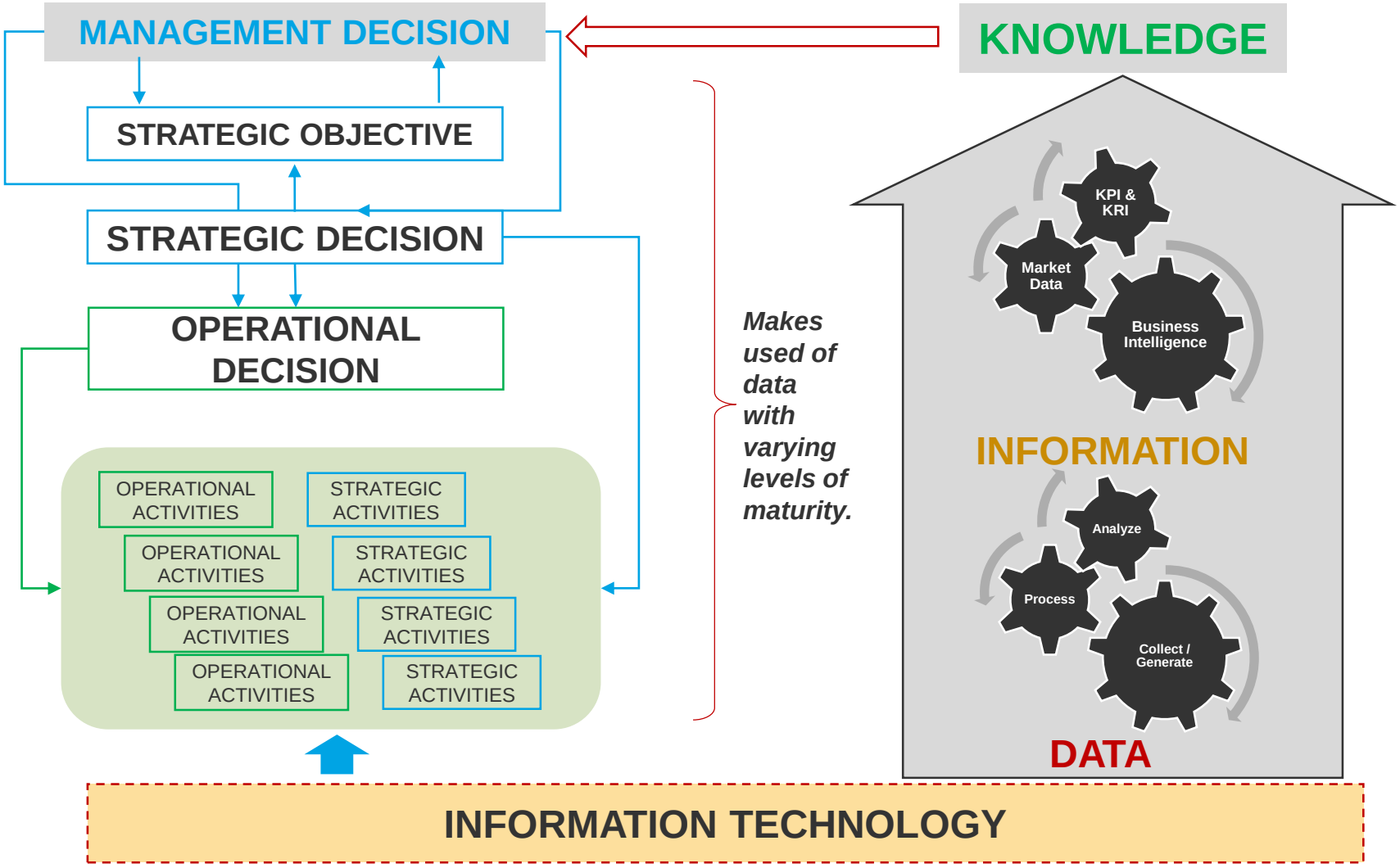
Who is accountable to address the below challenges?

- Culture, Vision & Strategy to include Cyber Security?
- Cyber strategy alignment with business strategy?
- Risk Management covering business technology needs and associated security implications.
- Risk appetite or tolerance?
- Validation of risk framework?
- Definition of Policies & Procedures?
- Alignment of Security spending with business objectives?
- Ongoing risk & security assessment?
- Implementation of required governance?

AIG

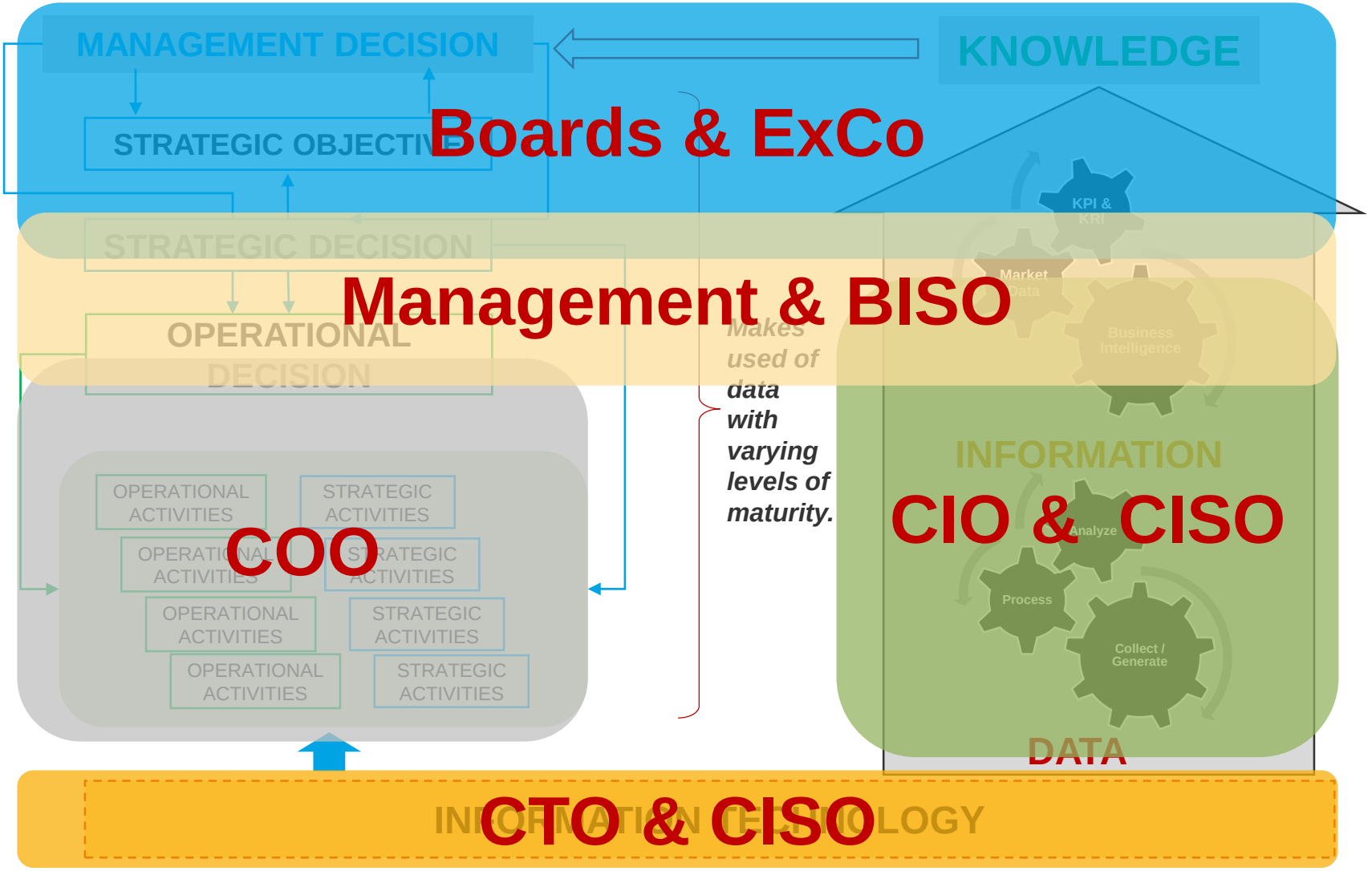
Cyber Resilience

Business, Technology…



Cyber Resilience

Business, Technology & Oversight Accountability…



Cyber Resilience

Best Practice for managing Cyber Risk

People

- Establish company culture to complement Digital Economy
- BOD ensure vision and strategy includes cyber security.
- Management to ensure cyber security is business strategy.
- Define Roles & Responsibilities for Cyber Security activities.

Process

- Risk management should integrated with day-to-day operations
- Practice relevant risk management process
- Implement a practical incident management, Crisis & DR plans.
- Implement checks & balances and segregation of duties.
- Identify & track IT assets. Assign ownership.

Technology

- Define & Implement security architecture & best practices.
- Minimize reliance on single security solution
- Track cyber security threats, trends & countermeasures
- Implement tools to analyze, identify and escalate security incidents.
- Develop forensic capability.

Governance

- Oversight & alignment BOD & Management.
- Security & Risk framework are reflective of business practice.
- Define metrics and track risk, audit and security activities for closure.
- Define Policies, Standards & SOP. Ensure compliance.
- Ensure security training for BOD, Management and general staff

AIG

Cyber Resilience

Board of Directors & Governance

Questions that company Directors should ask

1. What are the new cybersecurity threats and risks and how do they affect our organisation?
2. Is my organisation's cybersecurity program ready to meet the challenges of today's (and tomorrow's) cyber threat landscape?
3. What key risk indicators should I be reviewing at the executive management and board levels to perform effective risk management in this area?
4. Are cybersecurity aspects considered in our major business decisions, such as mergers and acquisitions, partnerships, new product launches?
5. Is there an ongoing, organisation-wide awareness and training program established around cybersecurity?
6. Are we confident that we will know if we have been hacked or breached, and what makes us certain that we will find out?

Red flags

- Cybersecurity is not on the boardroom agenda
- Cyber risk is not specifically included in assessing business and operational risk
- Specific accountability for cyber risk management, planning, and reporting is not defined
- Risks associated with cyber threats are not regularly reviewed and updated
- Organisational strategy and planning does not consider the changing nature of the online world and evolving cyber threats

3 OVERSIGHT OF TECHNOLOGY RISKS BY BOARD OF DIRECTORS AND SENIOR MANAGEMENT

3.0.1 IT is a core function of many FIs. When critical systems fail and customers cannot access their accounts, an FI's business operations may immediately come to a standstill. The impact on customers would be instantaneous, with significant consequences to the FI, including reputational damage, regulatory breaches, revenue and business losses.

3.0.2 In view of the importance of the IT function in supporting an FI's business, the board of directors and senior management should have oversight of technology risks and ensure that the organisation's IT function is capable of supporting its business strategies and objectives.

3.1 Roles and Responsibilities

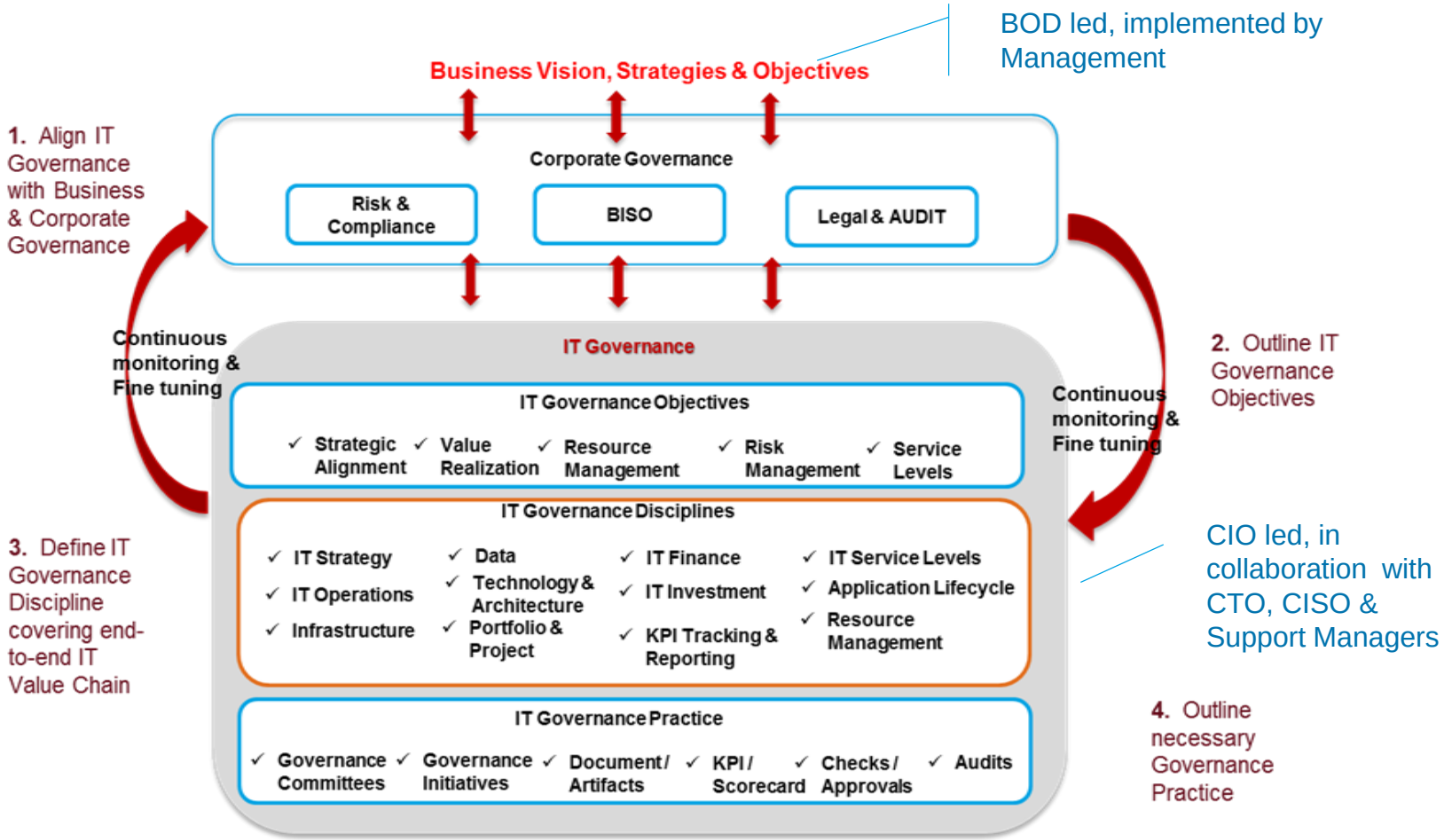
3.1.1 **The board of directors and senior management should ensure that a sound and robust technology risk management framework is established and maintained. They should also be involved in key IT decisions.** 3.1.2 They should also be fully responsible for ensuring that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability.

3.1.3 The board of directors and senior management should give due consideration to cost-benefit issues, including factors such as reputation, customer confidence, consequential impact and legal implications, with regard to investment in controls and security measures for computer systems, networks, data centers ("DC"), operations and backup facilities.

Source (Top): https://assets.kpmg.com/content/dam/kpmg/sg/pdf/2016/09/sg-Singapore-Directors-Toolkit.pdf
Source (Bottom): Technology Risk Management Guideline, Monitory Authority of Singapore

Cyber Resilience

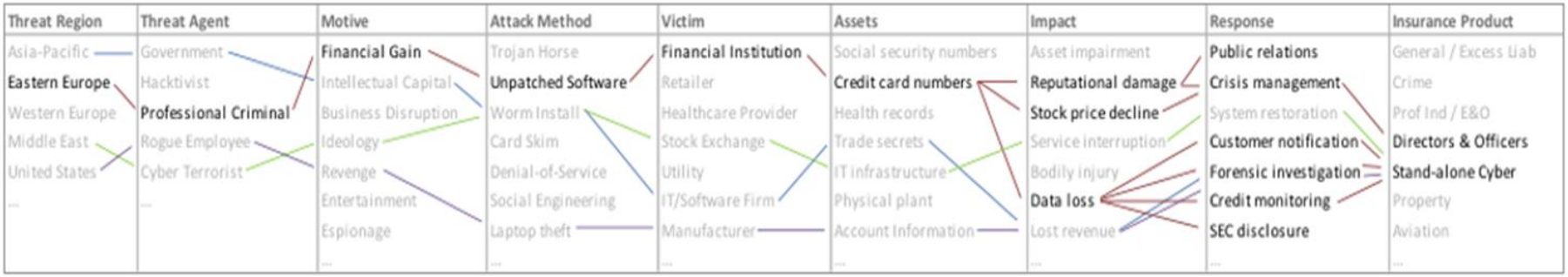
Implement effective Governance…



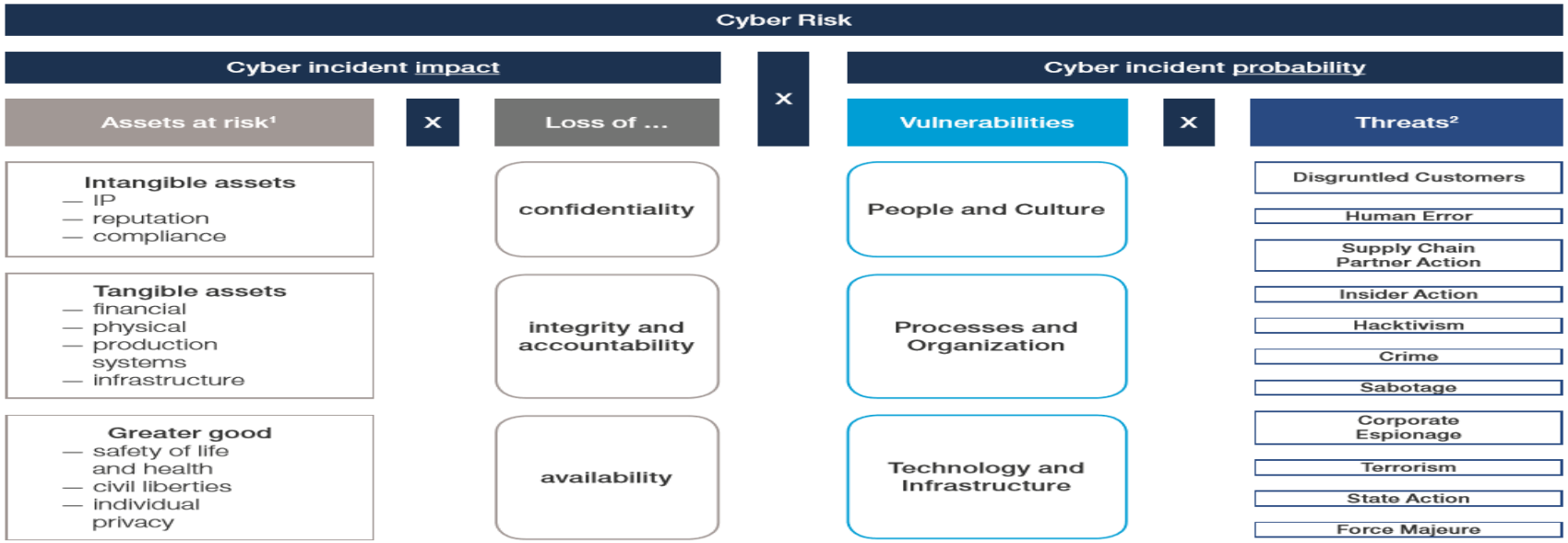
Cyber Resilience

Risk Framework…

- ✓ **BISO & Management** led exercise to identify and address Risk.
- ✓ Establish Framework to assess & identify **real & relevant** risk.



- ✓ Assess, Prioritize and Manage potential Risk.



Source AIG - Achieving Cyber Resilience

Cyber Resilience

Tips for Cyber Risk Mitigation...

CISO led exercise and managed by operational leads.

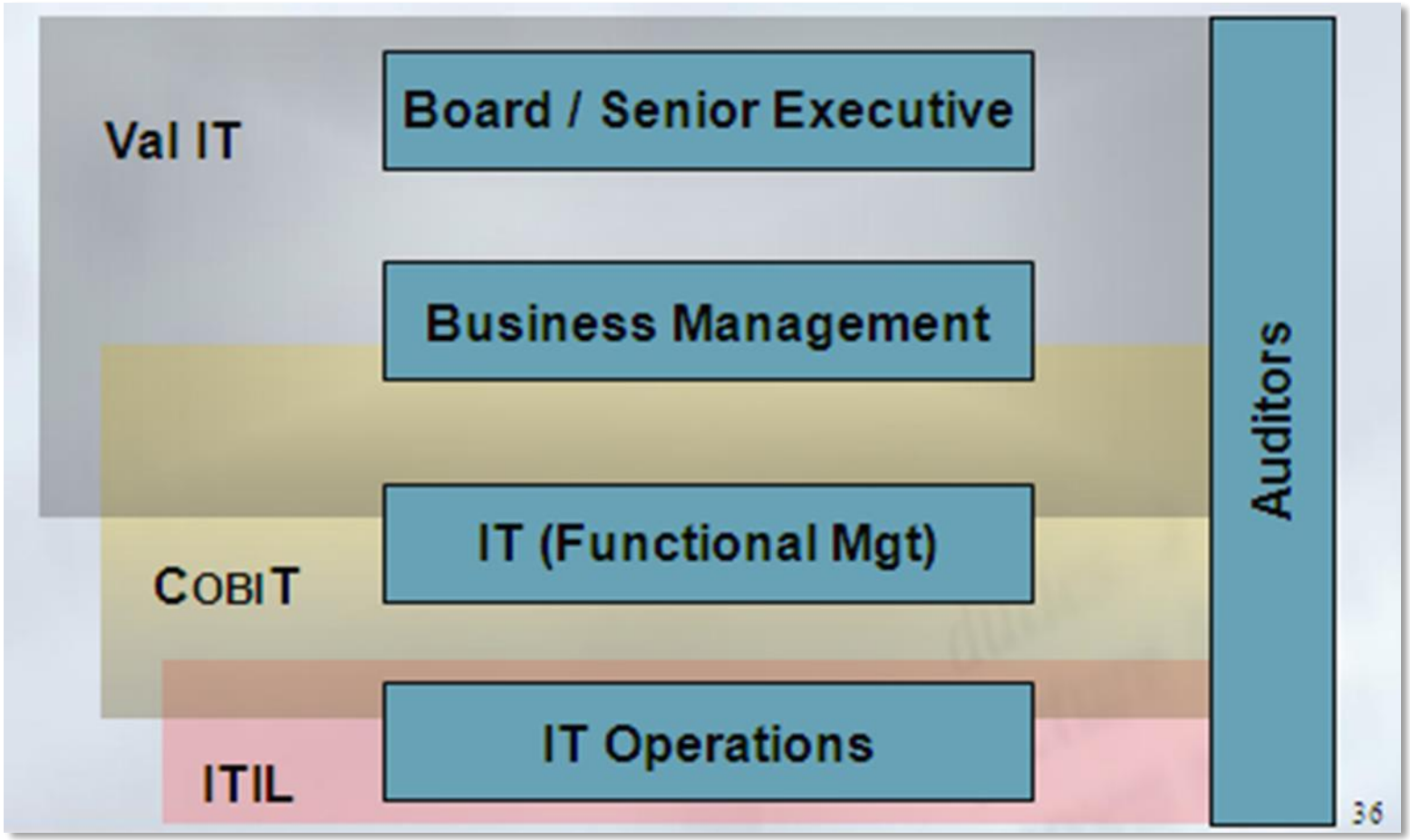
- Make an inventory of all IoT usage to help you better understand the scope of vulnerability.
- If the IoT platform comes with a default ID and password, change them. Attackers know these platforms and their defaults.
- When changing the password, consider using a “strong” password.
- Passwords should be changed regularly, and should remain complex, e.g. not a location, name, or other easily guessable user information.
- Practice a regular timely patch schedule and/or enable automatic updates and patching to occur if the IoT platform allows.
- Disable unnecessary remote administration and features.
- Do not allow unfiltered access to the device from the Internet; only allow whitelisted (trusted) connections via IP filtering or other security controls.
- Do not enable universal plug and play on IoT devices.
- Use secure protocols where possible, like HTTPS and SSH for device communications.
- Include IoT devices in regular vulnerability management programs
- Invest in CYBER Insurance

AIG

Source: https://www.aig.com/knowledge-and-insights/k-and-i-article-10-tips-for-cyber-risk-mitigation

Cyber Resilience

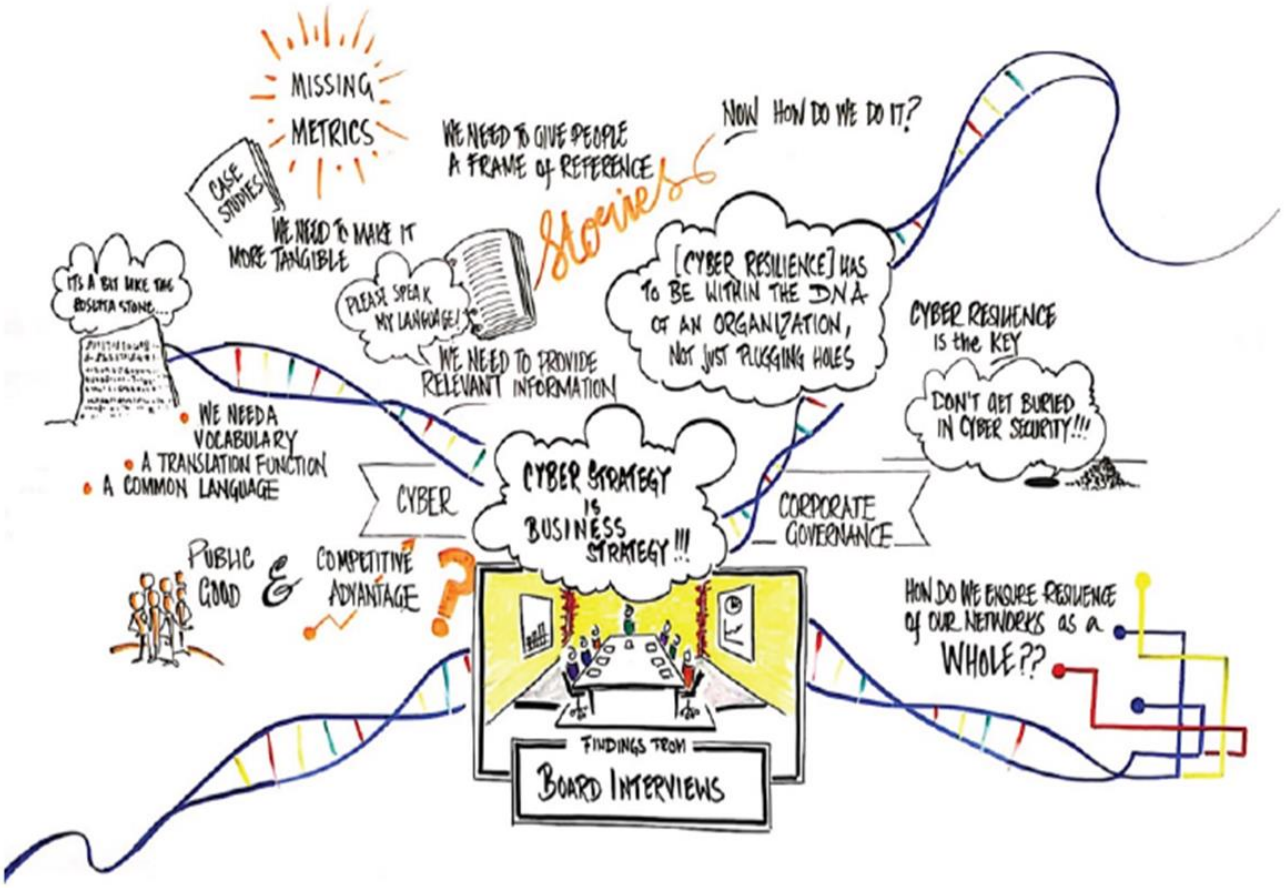
Governance Framework, What fits where?



Source: https://www.isaca.org/pages/default.aspx

Cyber Resilience

Cyber Strategy is Business Strategy…



A brainstorming session on board principles with the World Economic Forum Working Group on Cyber Resilience

RADHEY SHYAM

Chief Operating Officer
APAC IT

- Over 25 years of IT management experience.
- Over 17 years with AIG. Present responsibility includes:
  - IT Strategy, Investment & Finance Management, PMO
  - IT Operations & Services delivery
  - IT Risk Management, Security, Compliance & Regulatory
  - IT Governance & Vendor management.
- Held CIO responsibilities for Singapore & South Korea regions.

AIG