Why Cybersecurity needs to be a topic of boardroom agenda

Raj Kumar

Why Cybersecurity needs to be a topic of boardroom agenda

- Set management direction and gain support
- Understand business risk
- Protect brand and reputation
- Meet Legal and regulatory requirements
- Implement security awareness
- Allocate Budget and resources
- Establish organisation structure
- Foster collaboration between business units and technology team
- Develop strategic response to cyber threats

Impact of cyber threats on business profitability

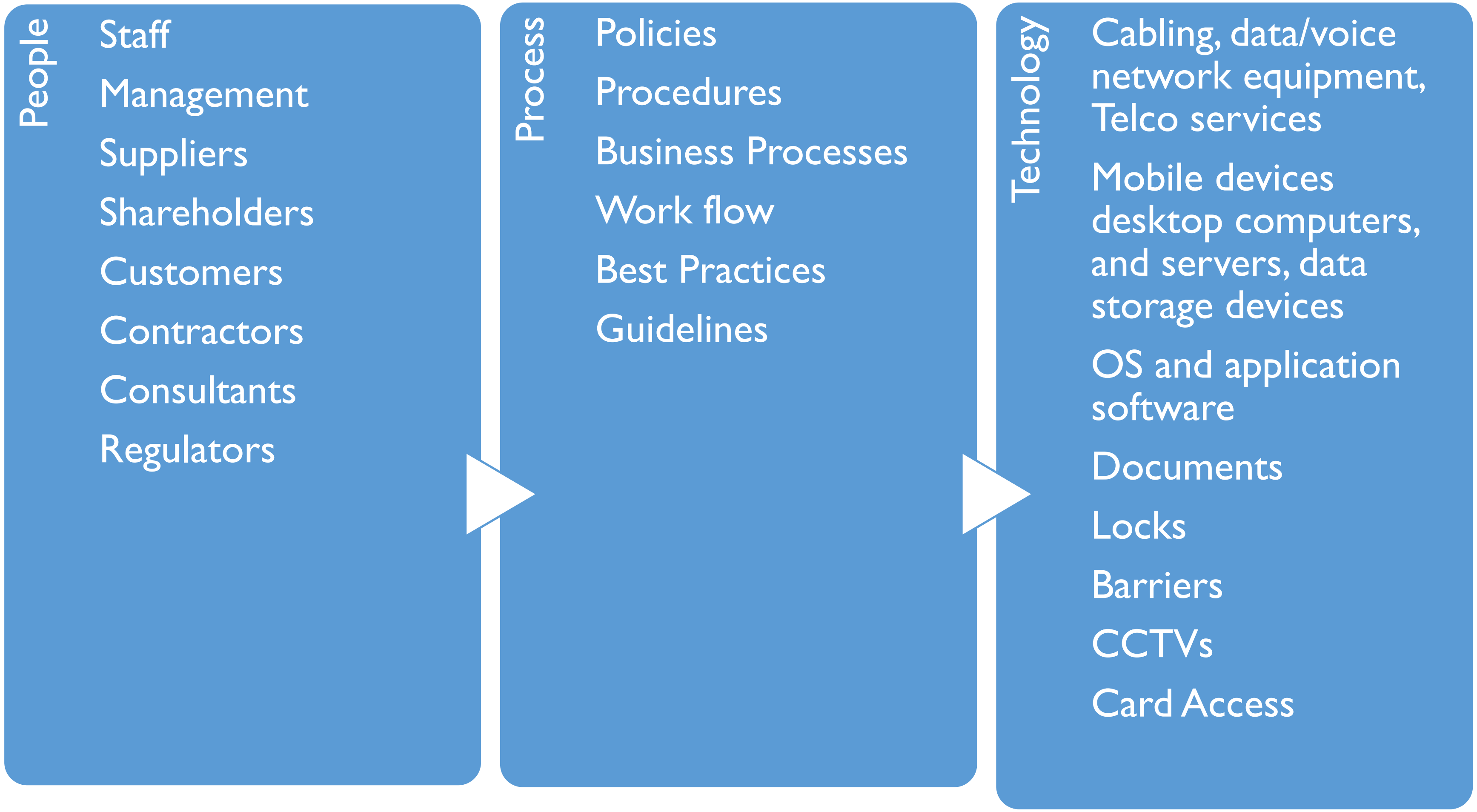
- Information security is what keeps valuable information asset ‘free of danger’ or threat

- Businesses need to:
    - Know what are the threat and vulnerabilities that can affect their business
    - Treat and manage the risk to information and physical asset
    - Ensure confidentiality, integrity and availability is preserved
    - Avoid, prevent, detect and recover from incidents
    - Securing people, processes *and* technology that are used
    - Protect the interest of customers, shareholders and partners
    - Business case to convince the senior management to invest and allocate resources for security management

Why Cyber security a must for business

- To protect brand and reputation
- To protect customer’s confidential information
- To ensure accuracy and correctness of information
- To ensure availability of information and system
- To meet legal and regulatory requirements
- To raise customer and third party confidence
- To understand risks and manage incidents
- To ensure business continuity and manage crisis

Core elements of cybersecurity for businesses



People

- Staff
- Management
- Suppliers
- Shareholders
- Customers
- Contractors
- Consultants
- Regulators

Process

- Policies
- Procedures
- Business Processes
- Work flow
- Best Practices
- Guidelines

Technology

- Cabling, data/voice network equipment, Telco services
- Mobile devices desktop computers, and servers, data storage devices
- OS and application software
- Documents
- Locks
- Barriers
- CCTVs
- Card Access

Definition: Resilience and Cyber - Resilience

Resilience

ITU-T SG17 defines resilience as the "Ability to recover from security compromises or attacks." Complementing this focus, a recent ITU report on 'Resilient Pathways' defines resilience as "*The ability of a system or a sector to withstand, recover, adapt, and potentially transform in the face of stressors such as those caused by climate change impacts*".

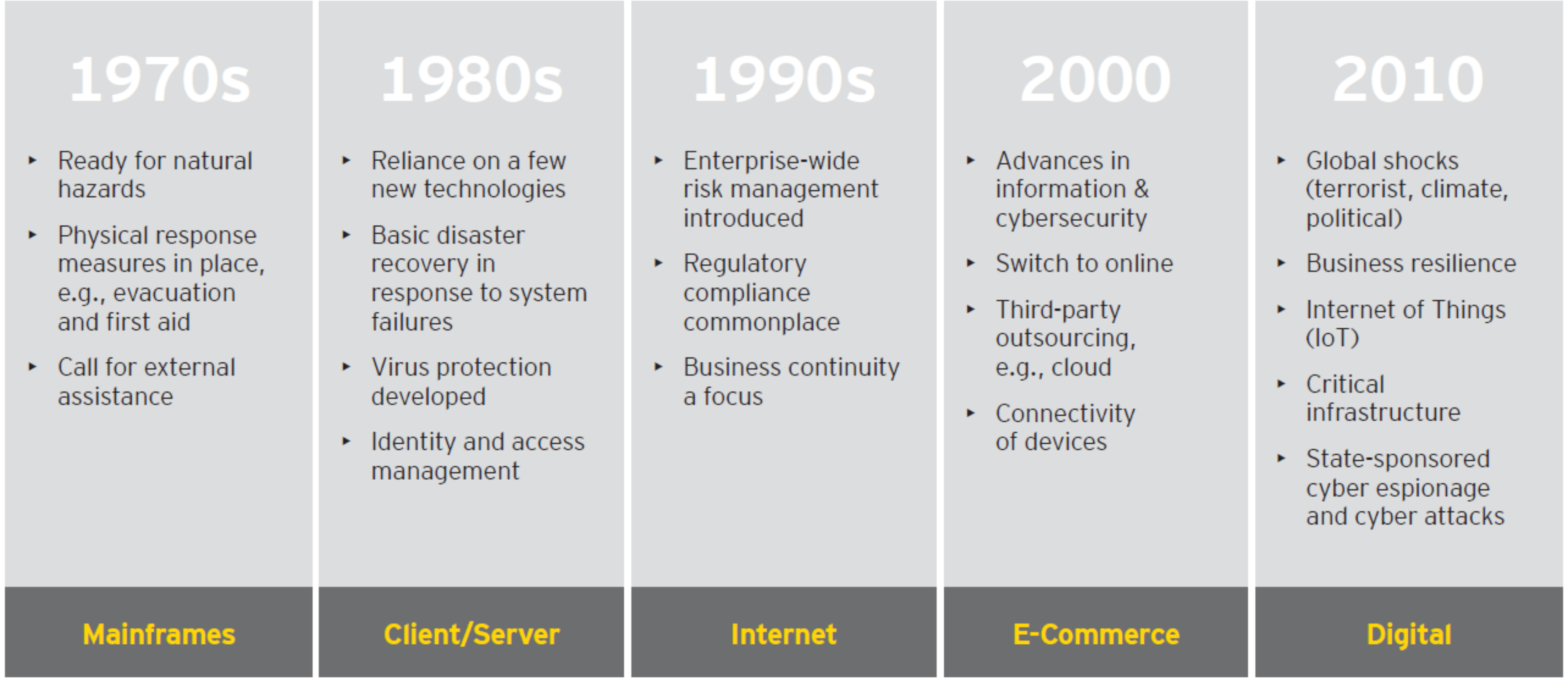
b. Cyber - security

This concept refers to the discipline of ensuring that ICT systems are protected by attacks and incidents, whether malicious or accidental, threatening the integrity of data, their availability or confidentiality, including attempts to illegally 'exfiltrate' sensitive data or information out of the boundaries of an organisation.

c. Data protection

This notion refers to the tools and processes used to store data relevant to a certain ICT system or environment, as well as recover lost data in case of an incident - be it fraudulent, accidental or caused by a natural disaster.

Definition: Resilience and Cyber - Resilience

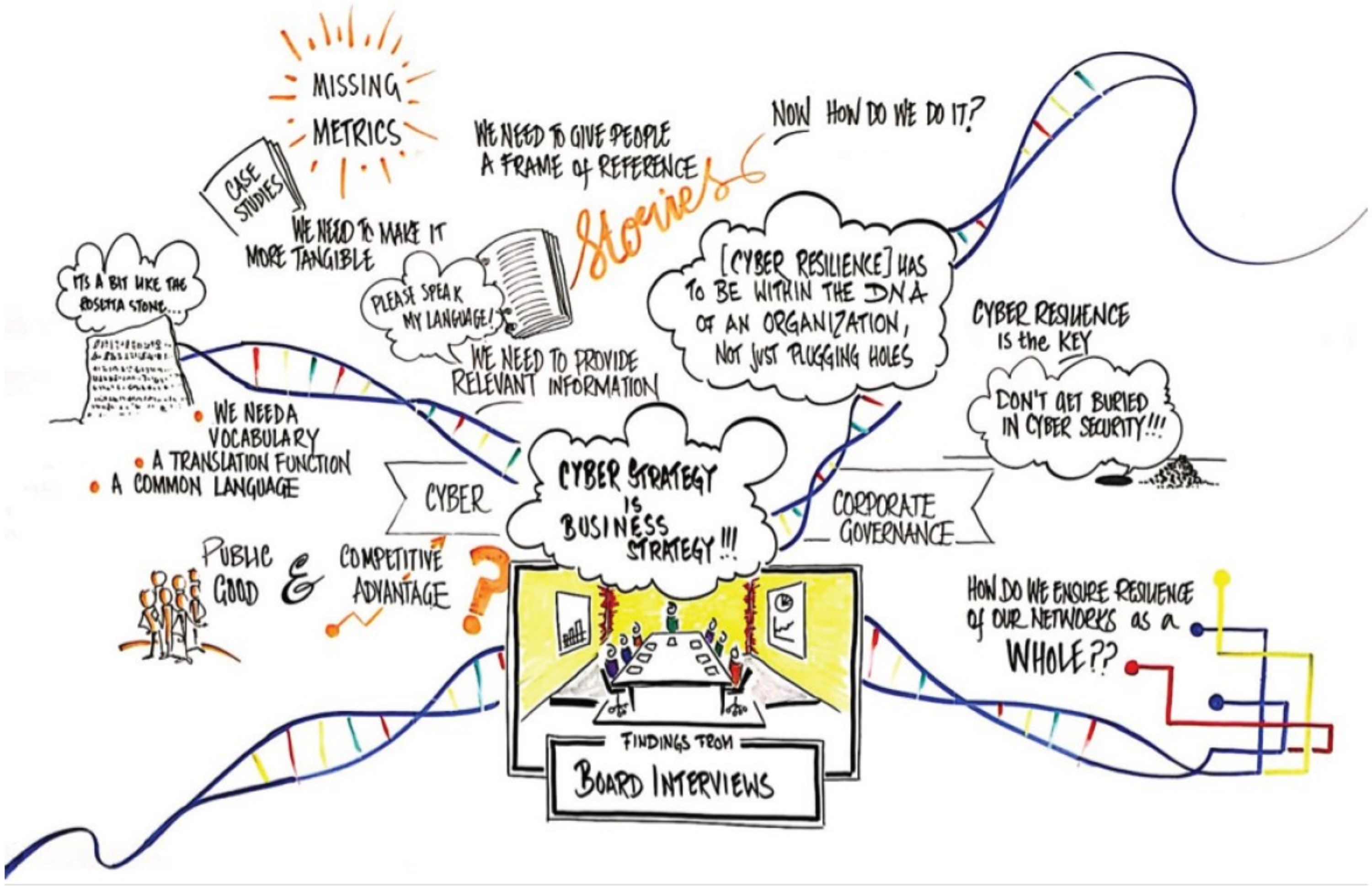


1970s	1980s	1990s	2000	2010
- Ready for natural hazards - Physical response measures in place, e.g., evacuation and first aid - Call for external assistance	- Reliance on a few new technologies - Basic disaster recovery in response to system failures - Virus protection developed - Identity and access management	- Enterprise-wide risk management introduced - Regulatory compliance commonplace - Business continuity a focus	- Advances in information & cybersecurity - Switch to online - Third-party outsourcing, e.g., cloud - Connectivity of devices	- Global shocks (terrorist, climate, political) - Business resilience - Internet of Things (IoT) - Critical infrastructure - State-sponsored cyber espionage and cyber attacks
Mainframes	Client/Server	Internet	E-Commerce	Digital

Cyber Resilience is the subset of business resilience

Source: EY-global-information-security-survey-2016-pdf

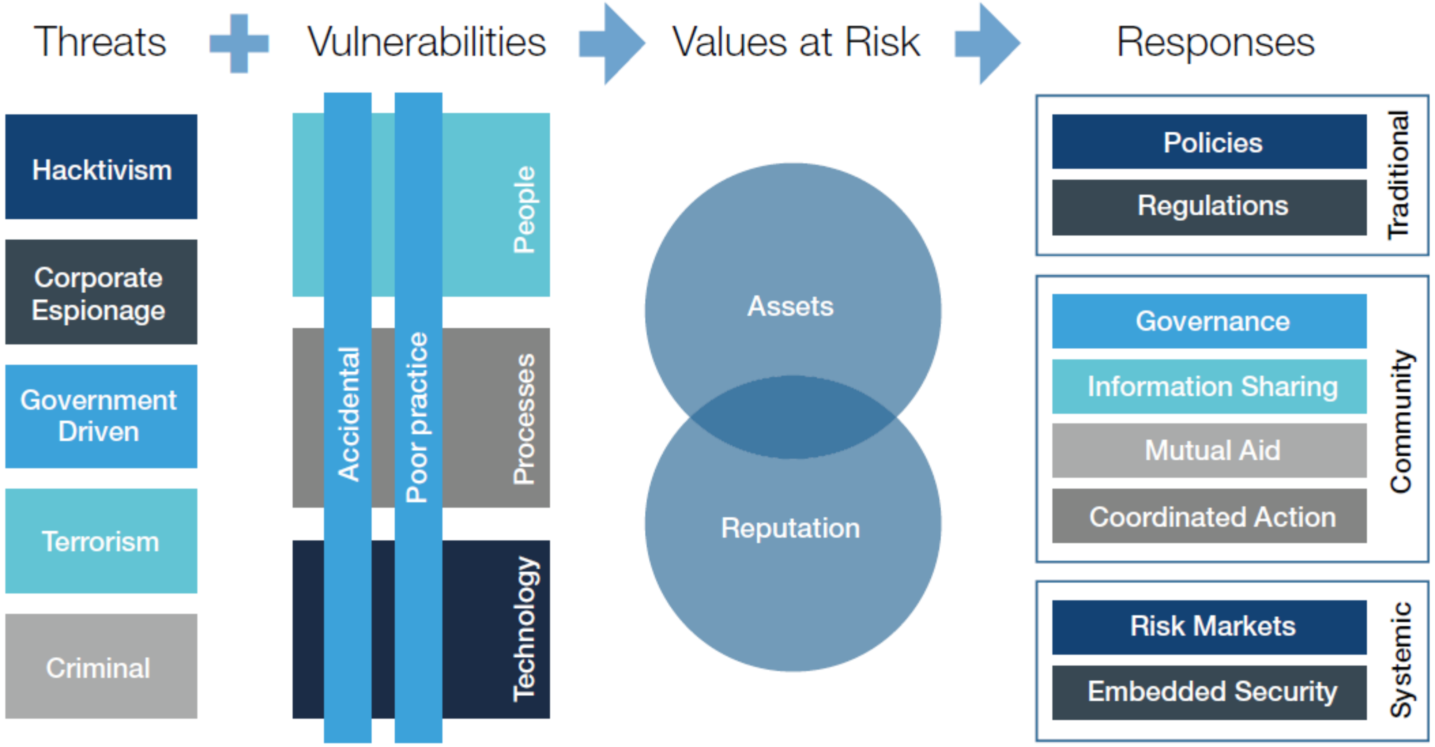
Ensuring resilience


MISSING METRICS
CASE STUDIES
WE NEED TO GIVE PEOPLE A FRAME OF REFERENCE
NOW HOW DO WE DO IT?
Stories
WE NEED TO MAKE IT MORE TANGIBLE
IT'S A BIT LIKE THE ROSETTA STONE...
PLEASE SPEAK MY LANGUAGE!
WE NEED TO PROVIDE RELEVANT INFORMATION
[CYBER RESILIENCE] HAS TO BE WITHIN THE DNA OF AN ORGANIZATION, NOT JUST PLUGGING HOLES
CYBER RESILIENCE IS the KEY
DON'T GET BURIED IN CYBER SECURITY!!!
WE NEED A VOCABULARY
A TRANSLATION FUNCTION
A COMMON LANGUAGE
CYBER
CYBER STRATEGY IS BUSINESS STRATEGY!!!
CORPORATE GOVERNANCE
PUBLIC GOOD & COMPETITIVE ADVANTAGE ?
HOW DO WE ENSURE RESILIENCE of OUR NETWORKS as a WHOLE??
FINDINGS FROM BOARD INTERVIEWS

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

ITU-D 1992 2017 CELEBRATING 25 YEARS OF ACHIEVEMENTS

Cyber Risk Framework



Source: WEF IT Partnering Cyber Resilience Guidelines 2012

From the board room

We need to develop a coherent cyber resilience strategy

We need to know what our critical information assets are

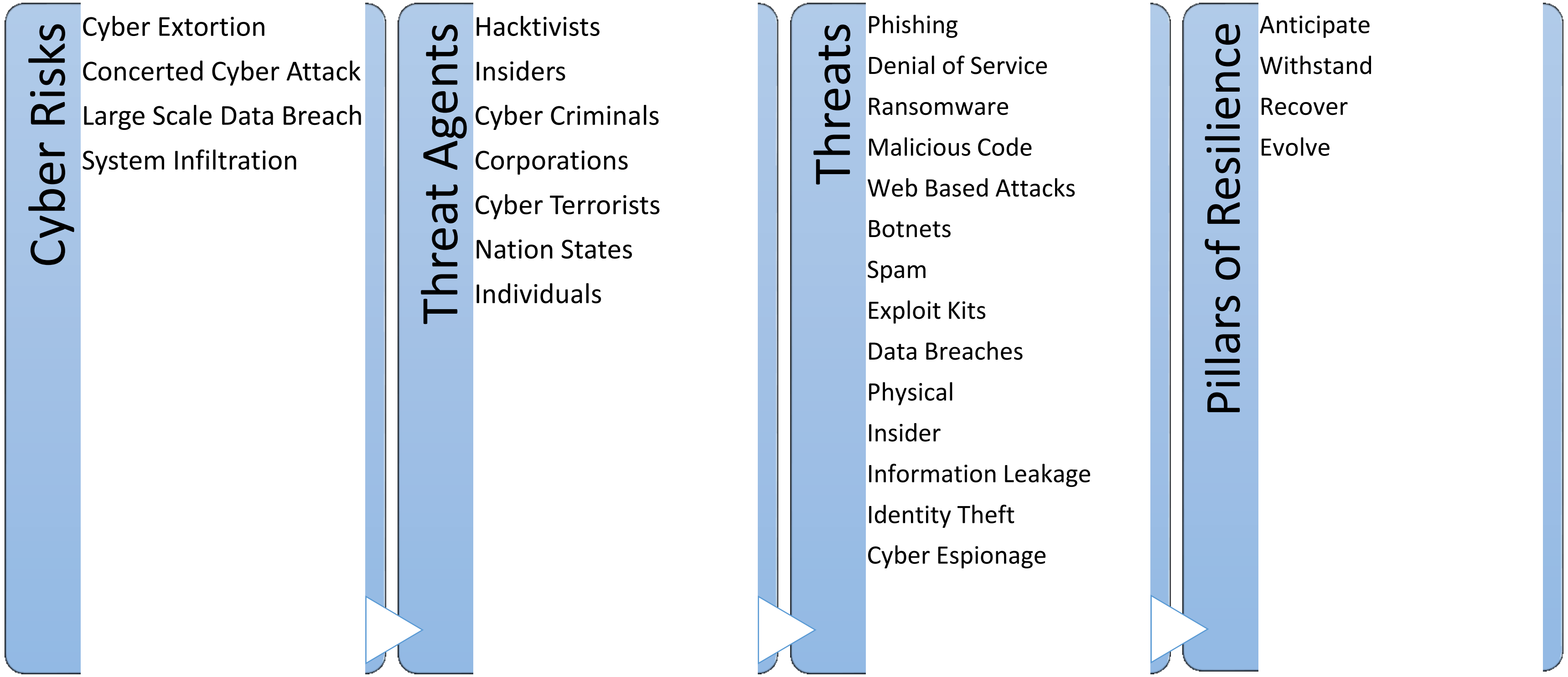
We need a cyber smart workforce and partner network

We need to embed good practices across our organization

We need to communicate and understand more effectively across the organization

We need to understand how we will respond and recover from attack more effectively

Ensuring resilience



Cyber Risks

- Cyber Extortion
- Concerted Cyber Attack
- Large Scale Data Breach
- System Infiltration

Threat Agents

- Hacktivists
- Insiders
- Cyber Criminals
- Corporations
- Cyber Terrorists
- Nation States
- Individuals

Threats

- Phishing
- Denial of Service
- Ransomware
- Malicious Code
- Web Based Attacks
- Botnets
- Spam
- Exploit Kits
- Data Breaches
- Physical
- Insider
- Information Leakage
- Identity Theft
- Cyber Espionage

Pillars of Resilience

- Anticipate
- Withstand
- Recover
- Evolve

3 high-level components of cyber resilience

Sense

Ability of organisation to detect cyber threats

Using cyber intelligence, analytics and active defence

Early warning of risk of disruption

Resist

Determine how much risk an organisation can take across its ecosystem

3 lines of defence

- Executing controls on daily operations
- Deploying monitoring function – internal controls, legal department, risk management
- Internal audit

React

If Sense fails, the organisation failed to see the threat coming, there is a breakdown in React (the controls were not strong enough

Organisation need to be ready for disruption

Ready with incident response capabilities

Ready to manage crisis

Ready to preserve evidence

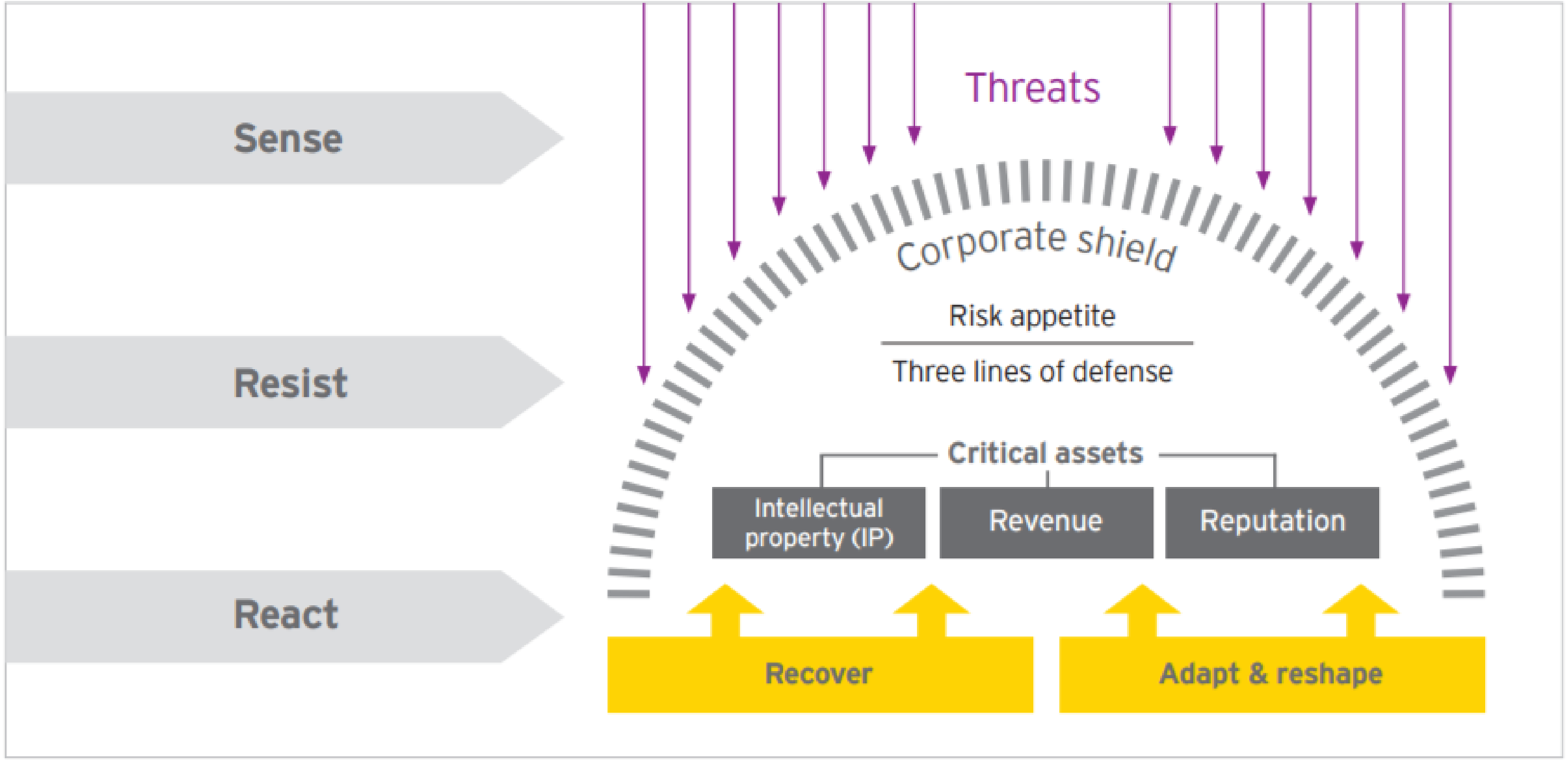
Investigate the breach to satisfy customers, regulators, investors, law enforcement and the public

Bring the business back to normal state

Learn form what happened and improve cyber resilience.

Source: EY-global-information-security-survey-2016-pdf

Ensuring resilience



Source: EY-global-information-security-survey-2016-pdf

Ensuring resilience

	Sense (See the threats coming)	**Resist** (The corporate shield)	**React** (Recover from disruption)
Where do organizations place their priorities?	**Medium**	**High**	**Low**
Where do organizations make their investments?	**Medium**	**High**	**Low**
Board and C-level engagement	**Low**	**High**	**Low**
Quality of executive or boardroom reporting	**Low**	**Medium**	**Low**

CIS 20 Controls

Center for Internet Security

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

1) Inventory of Authorized and Unauthorized Devices

2) Inventory of Authorized and Unauthorized Software

3) Secure Configurations for Hardware and Software

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

10) Data Recovery Capability

11) Secure Configurations for Network Devices

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

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

With regard to Critical Security Controls, CSC "...failure to implement all of the controls that apply to an organization's environment constitutes a lack of reasonable security."
Kamala Harris, Attorney General, CA
Breach Report 2016

ITU : I Thank U

CELEBRATING 25YEARS OF ACHIEVEMENTS