Cyber Security – A Bird's Eye View

Frameworks and Solutions

Nandkumar Saravade

Cyber Security: A wicked problem

- …a problem that is difficult or impossible to solve because of incomplete, contradictory, and changing requirements that are often difficult to recognise.
- no single solution to the problem
- "wicked" denotes resistance to resolution, rather than evil
- complex interdependencies
- the effort to solve one aspect of a wicked problem may reveal or create other problems.

Diagnosing the Issue

The Tale of Maersk

- Fortune300 company/130 countries/88,000 employees/$39 billion revenue in 2020
- 75 port terminals (including JNPT), 780+ vessels
- 90% of global commerce via shipping
- Maersk handles 18% global container traffic
- Hit with NotPetya ransomware in 2017, only one powered-off computer in Ghana held a backup of the company data
- Back to basic: using paper and WhatsApp
- Final cost: $300 million

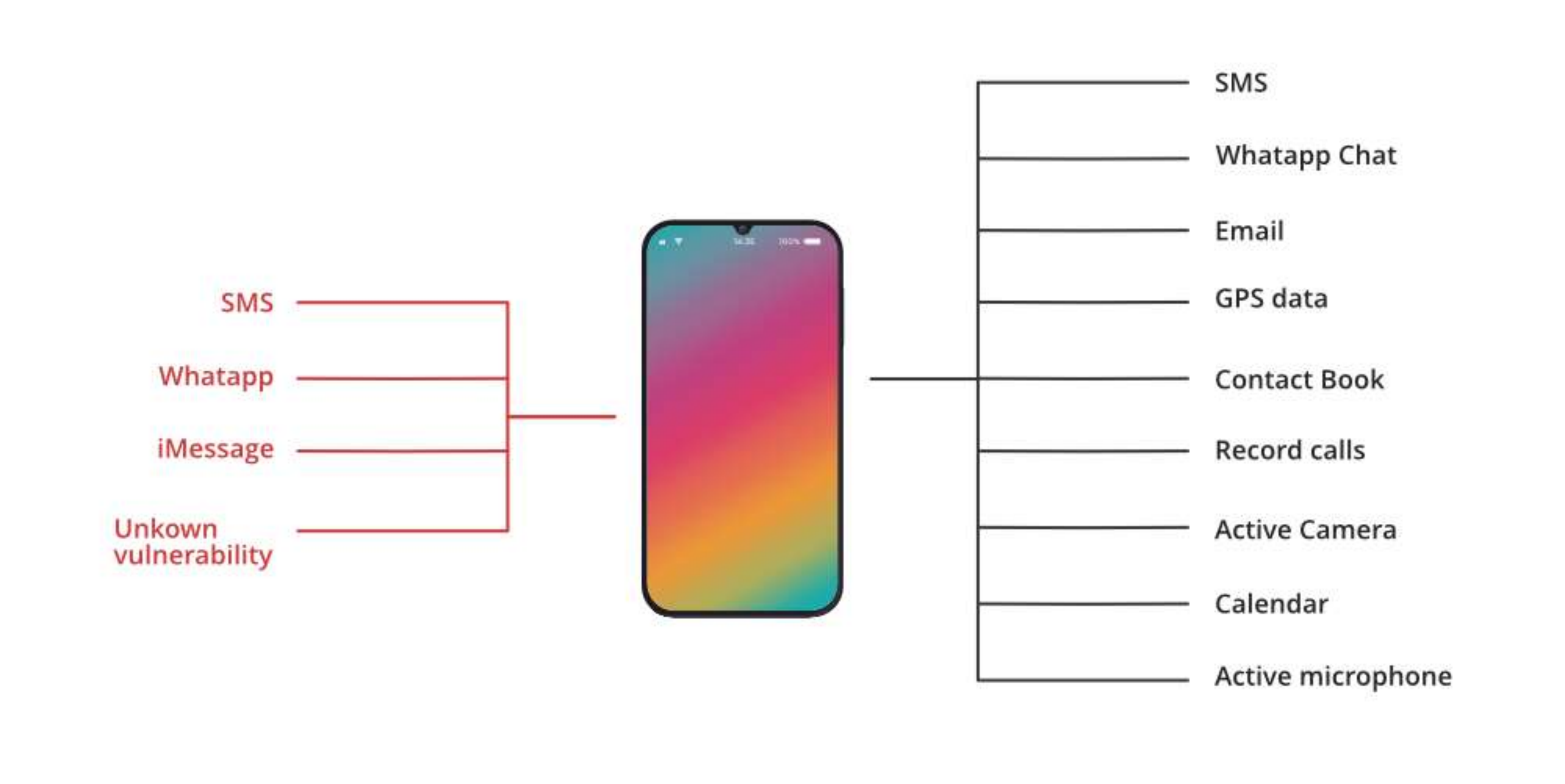
Brazilian Bank Hijack

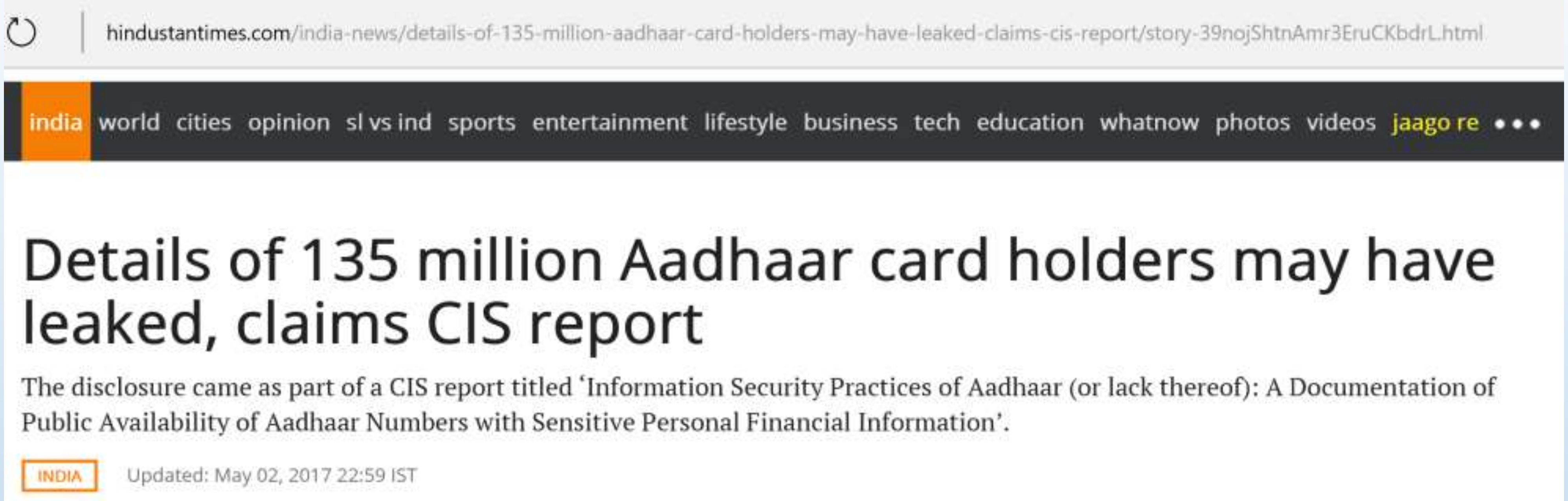
- One weekend afternoon (22-10-16), hackers compromised the bank's account at Registro.br and changed the Domain Name System registrations of all 36 of the bank's online properties
- Hundreds of branches, operations in the US and the Cayman Islands, 5 million customers, and more than $27 billion in assets
- Collected credentials of customers; downloaded malware as update to Trusteer; may have redirected ATM/PoS transactions too
- Certificates had been issued six months earlier by Let's Encrypt
- Bank was unable to send email to customers; had to call up the registrar
- Half of the top 20 banks ranked by total assets don't manage their own DNS

Recent Significant Cyber Incidents

- The Equifax hack: Compromise of 143 million records | Due to an unpatched vulnerability (2 month window) | Argentina portal with ‘admin’/’admin’ credentials | Poor response to the crisis
- SEC Electronic Data Gathering, Analysis, and Retrieval System (EDGAR) compromised ‘sometime in 2016’ | Detected in August 2017 | May have led to trading based on undisclosed information
- Deloitte mail server breach | $37bn revenue | Single Factor admin credentials
- Incidents: Union Bank of India/Bank of Maharashtra/Hitachi Payment/Ransomware/Aadhaar data exposure/ City Union Bank/Colonial Pipeline/Pegasus

What can Pegasus do?

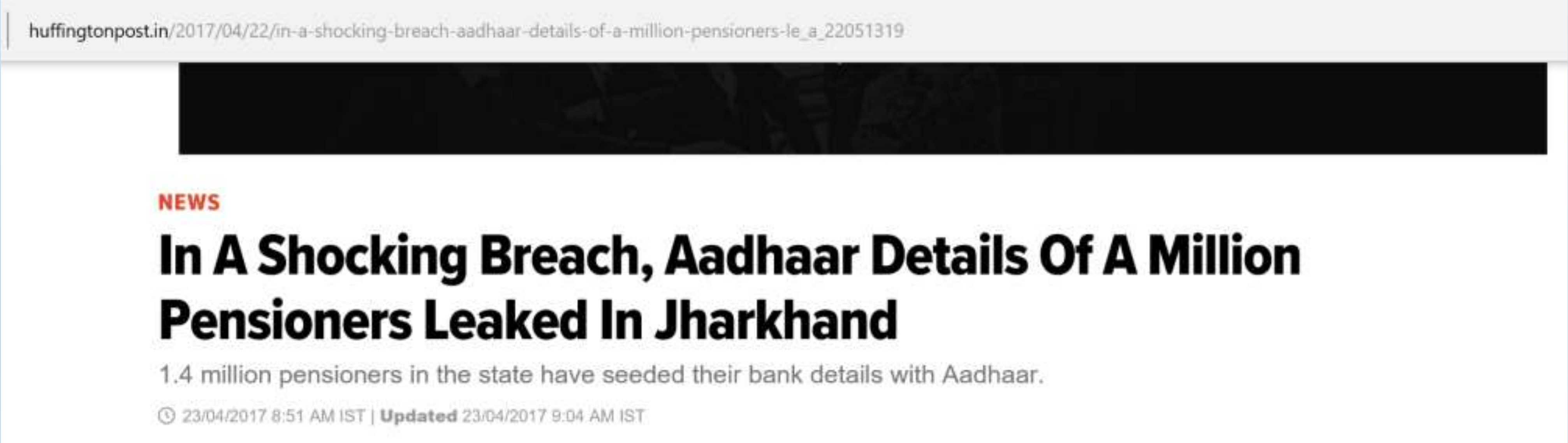



hindustantimes.com/india-news/details-of-135-million-aadhaar-card-holders-may-have-leaked-claims-cis-report/story-39nojShtnAmr3EruCKbdrL.html
india world cities opinion sl vs ind sports entertainment lifestyle business tech education whatnow photos videos jaago re

Details of 135 million Aadhaar card holders may have leaked, claims CIS report

The disclosure came as part of a CIS report titled 'Information Security Practices of Aadhaar (or lack thereof): A Documentation of Public Availability of Aadhaar Numbers with Sensitive Personal Financial Information'.

INDIA Updated: May 02, 2017 22:59 IST


huffingtonpost.in/2017/04/22/in-a-shocking-breach-aadhaar-details-of-a-million-pensioners-le_a_22051319

NEWS

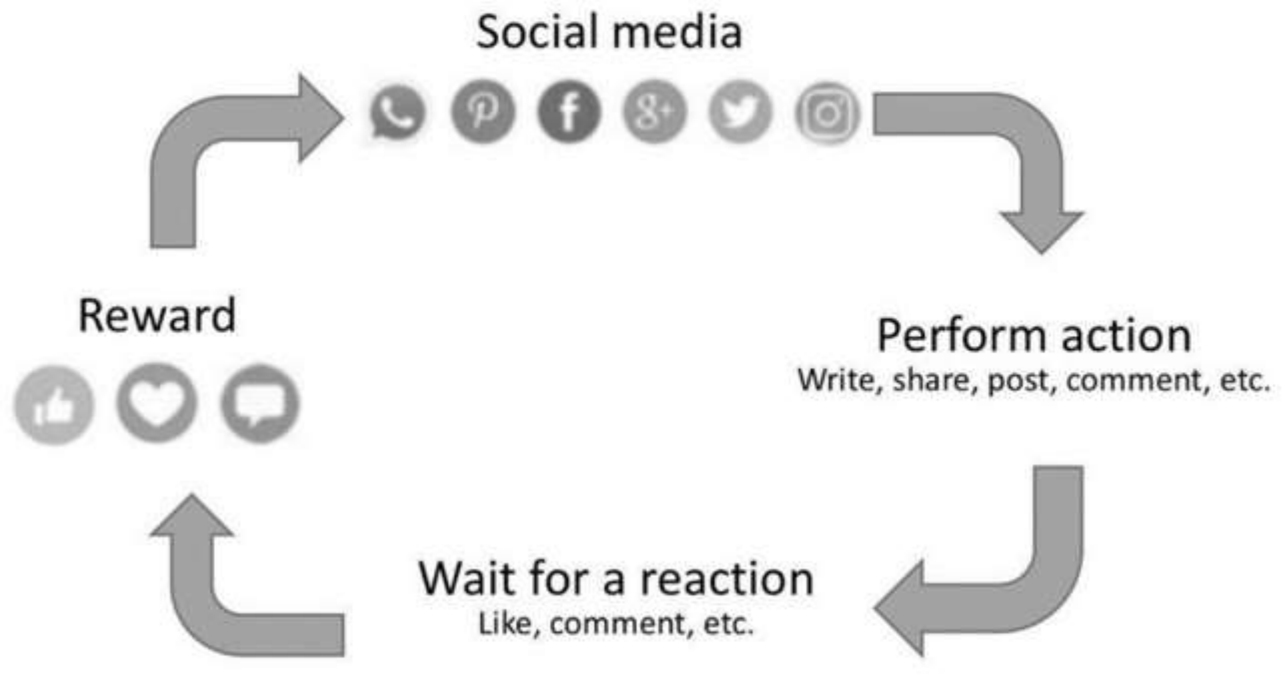
In A Shocking Breach, Aadhaar Details Of A Million Pensioners Leaked In Jharkhand

1.4 million pensioners in the state have seeded their bank details with Aadhaar.

23/04/2017 8:51 AM IST | **Updated** 23/04/2017 9:04 AM IST

Is Social Media killing democracy?

- “A lie can travel halfway around the world while the truth is putting on its shoes.”
- One upside/downside of the Web is everyone has a printing press.
- The Dopamine Merchants
- What is visible (Facebook) and what is not (WhatsApp).



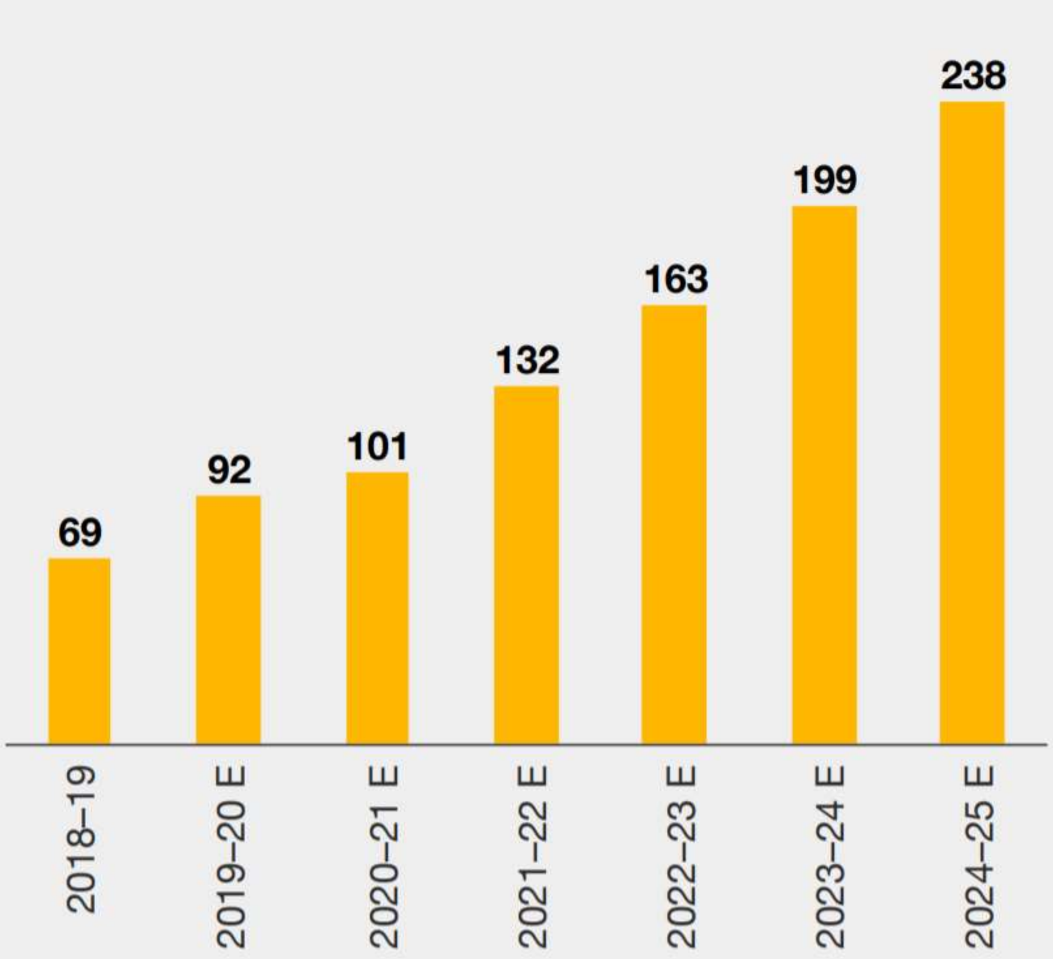
Tech Trends: Global/Local

Digital Trends in India

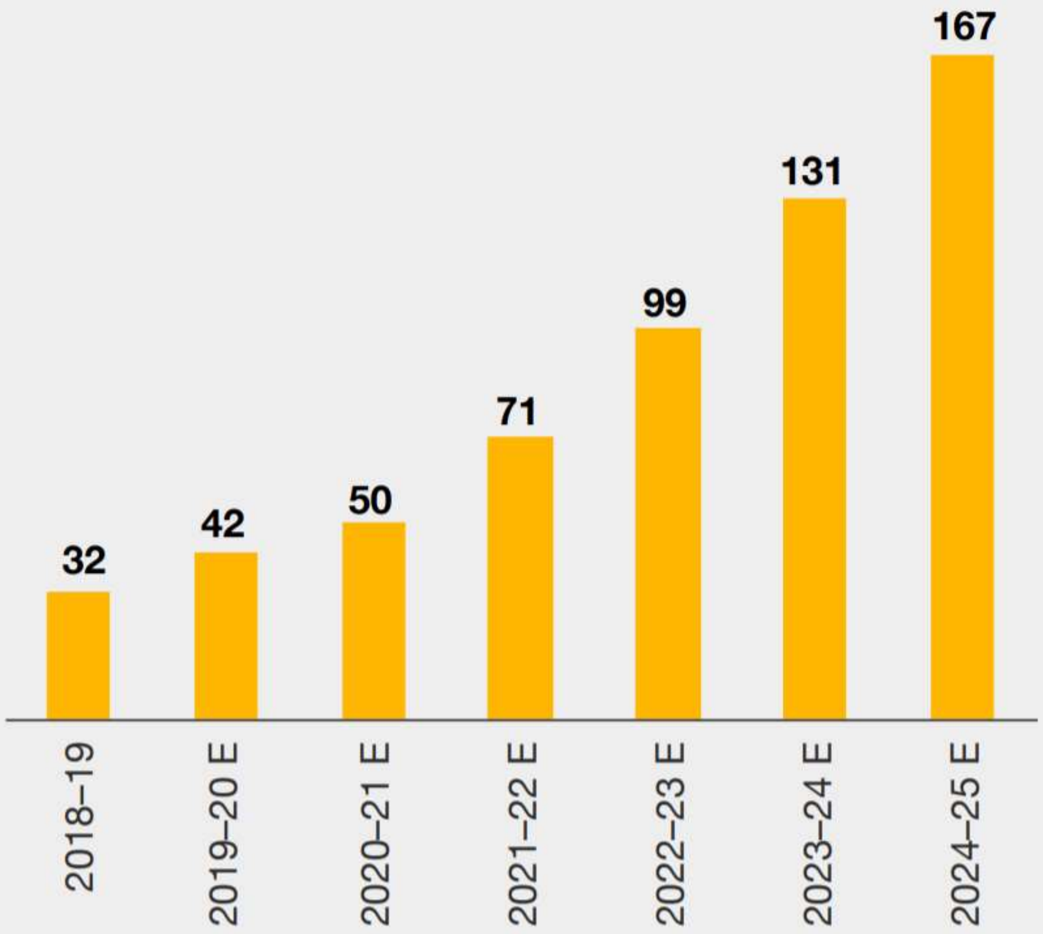
- Impressive achievements
  - Financial inclusion: Jan Dhan Accounts 30.38 crore | 22.89 crore RuPay cards | UPI payment system
  - Communications: Mobile phones 948 million
  - Internet users >42 crore | Urban @52%/Rural @16%
  - Aadhaar enrolments: Crossed 1 billion
  - Ambitious Smart Cities Programme (> ₹2 lakh crore)
  - Digital Commerce (> ₹2.2 lakh crore)

- Social Media use in India
  - The number of social media users in India were 376.1 million in 2020
  - The number of users is expected to cross 448 million by 2023.
  - Facebook is the most used social media platform in India, with around 86% traffic.
  - Indian social media users downloaded 19 billion apps in 2019 alone
  - There has been a 195% growth in downloaded apps in India since 2016

Value and volume of digital transactions in India



Transaction value (in INR trillion)



Transaction volume (in billion)

Source: PwC analysis of RBI data

Frameworks

> “When a resource becomes essential to competition but inconsequential to strategy, the risks it creates become more important than the advantages it provides.”

-- *Nicholas Carr*

Some Basic Concepts

- How does the computer know you?
  - Knowledge / Possession/ Inherence
- PPT: People / Process / Technology
- Vulnerabilities/Threats/Incidents
- What is at stake?
  - Confidentiality/Integrity/Availability/Safety
- Security Framework: Prevent / Detect / Respond
- Risk Management
  - Assessment
  - Avoid / Mitigate / Transfer / Accept

What is special about cyber risk?

- There are adversaries on the other side
    - Operating in a developed market place/innovative/with global allies/tolerated or nurtured by nation states
- Increasing attack frequency + diminishing technology cost
- Adaptive and dynamic, complicating risk assessment
- Attribution challenges, amid low cross-border collaboration
- The true aggregation of risks goes well beyond the internal monitoring and risk management capacities of individual institutions
- 90 percent of the total costs are attributable to indirect factors /True cost of cyber-attacks manifests only over several years

Cyber Crime: What’s new?

- Remote access
  - Proximity of the perpetrator and the victim no longer necessary
- Trivial transaction costs
- Difficulties in apprehension
  - Anonymising services
  - Public access points/scattered scenes of crime
  - Sheer number of users/identities/devices
  - Jurisdictional arbitrage
- Unlegislated criminal behaviour
- Scale of operations
  - Serial crime replaced by parallel crime
  - Asymmetric advantage to the attacker

Safe Havens: Have you seen these persons?

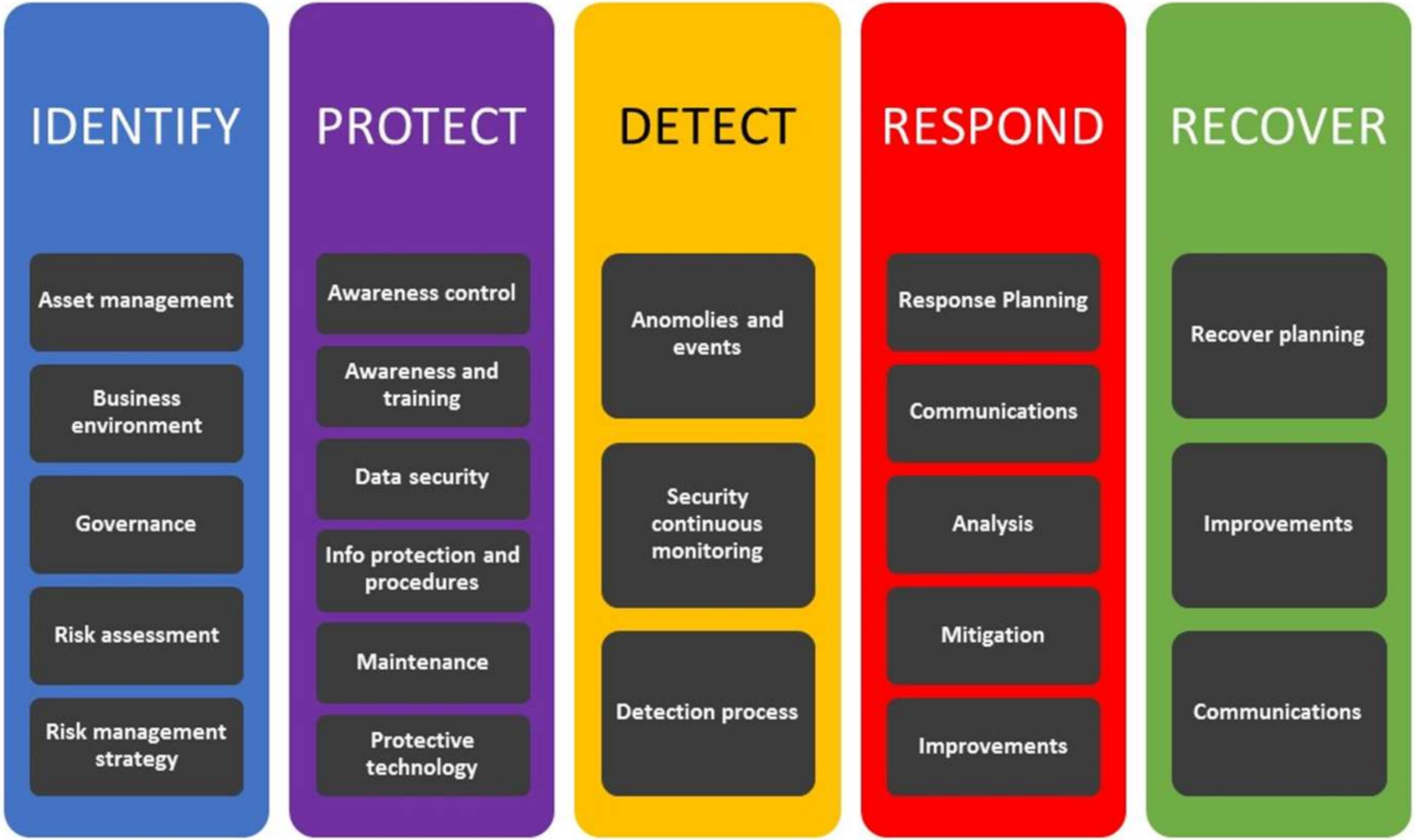
Importance of the eco-system

- Who detects?
  - Employees: 50%
  - Law enforcement: 25%
  - Customers: 21%
  - Service providers: 19%
- Ross Anderson et al: “the botnet behind a third of the spam sent in 2010 earned its owners around $2.7m, while worldwide expenditures on spam prevention probably exceeded a billion dollars.”
- “Cybercrooks are like terrorists or metal thieves in that their activities impose disproportionate costs on society.”
- “We should spend less in anticipation of cybercrime (on antivirus, firewalls, etc.) and more in response – that is, on the prosaic business of hunting down cyber-criminals and throwing them in jail.”

The Issue of Privacy

- SC: Privacy as a fundamental right
  - Expert committee appointed by MeitY, under Justice Srikrishna; Draft Published; Public consultation carried out
- Lack of awareness about the concept of privacy in India
  - The Aadhaar Act: Section 29(4) *No Aadhaar number or core biometric information collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations.*
- OECD Privacy Principles
  - Notice—data subjects should be given notice when their data is being collected;
  - Purpose—data should only be used for the purpose stated and not for any other purposes;
  - Consent—data should not be disclosed without the data subject’s consent;
  - Security—collected data should be kept secure from any potential abuses;
  - Disclosure—data subjects should be informed as to who is collecting their data;
  - Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
  - Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.

NIST Cybersecurity Framework



IDENTIFY
- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

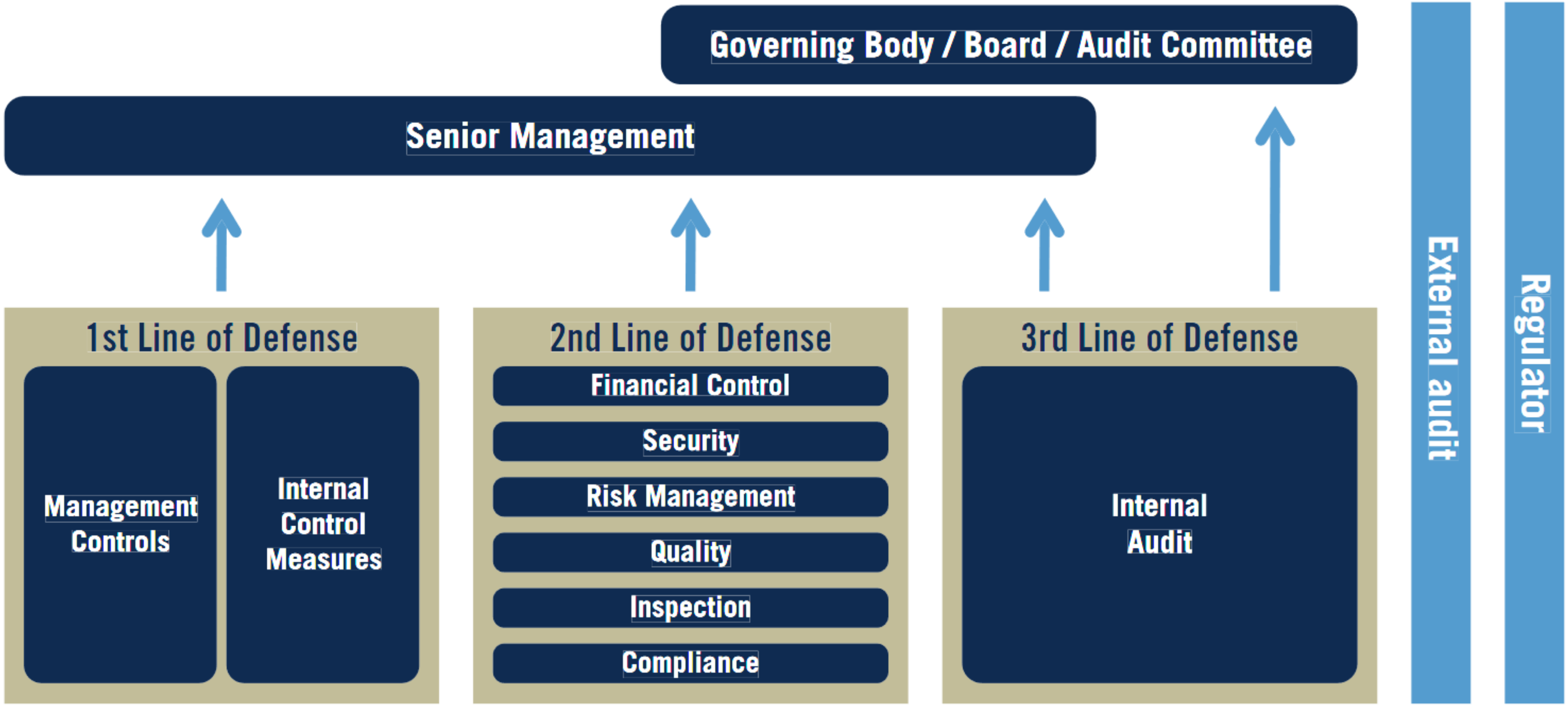
PROTECT
- Awareness control
- Awareness and training
- Data security
- Info protection and procedures
- Maintenance
- Protective technology

DETECT
- Anomolies and events
- Security continuous monitoring
- Detection process

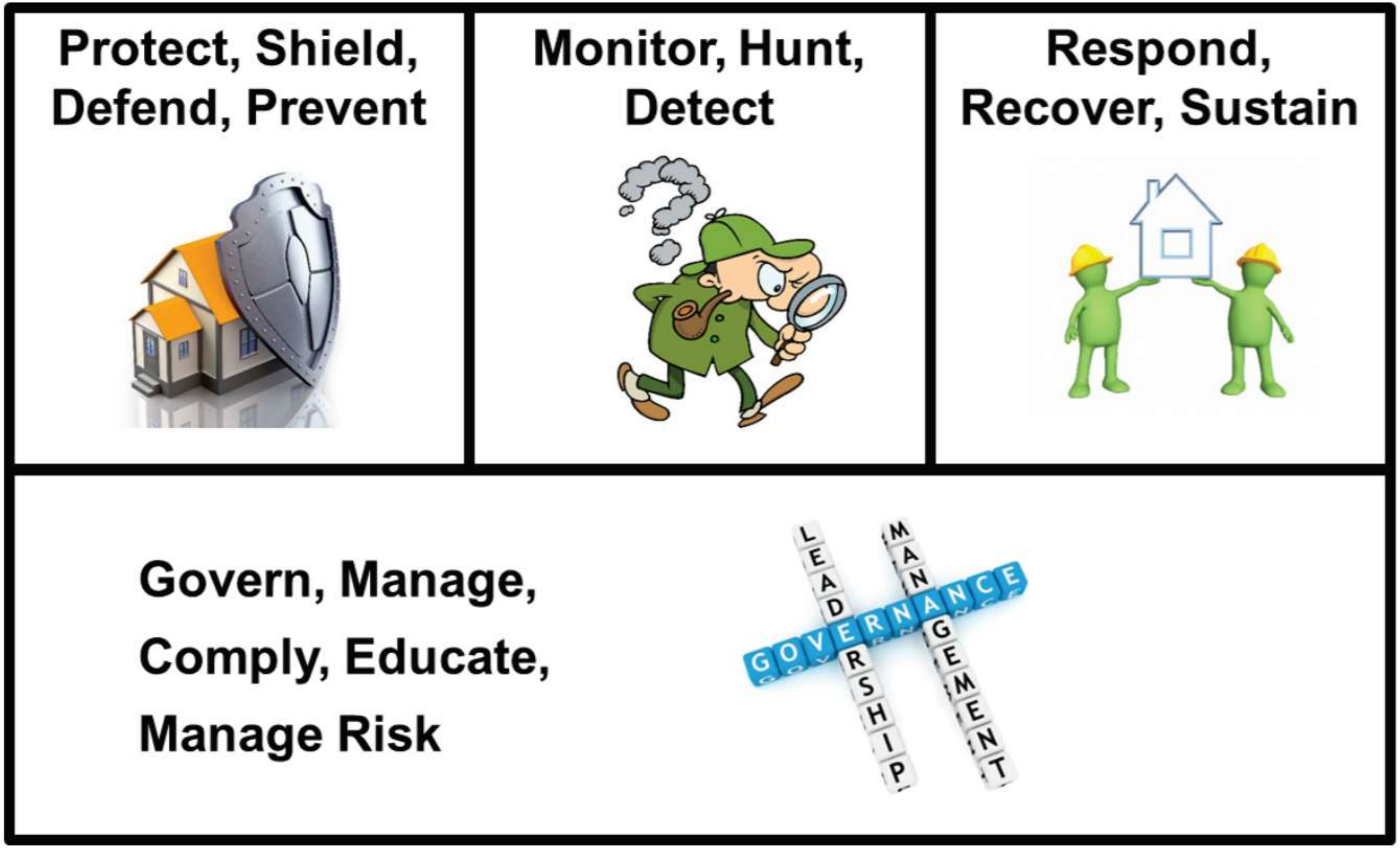
RESPOND
- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER
- Recover planning
- Improvements
- Communications

The Three Lines of Defense Model



Adapted from ECIIA/FERMA *Guidance on the 8th EU Company Law Directive, article 41*



Protect, Shield, Defend, Prevent

Monitor, Hunt, Detect

Respond, Recover, Sustain

Govern, Manage, Comply, Educate, Manage Risk

Figure 1: Four CISO Functions

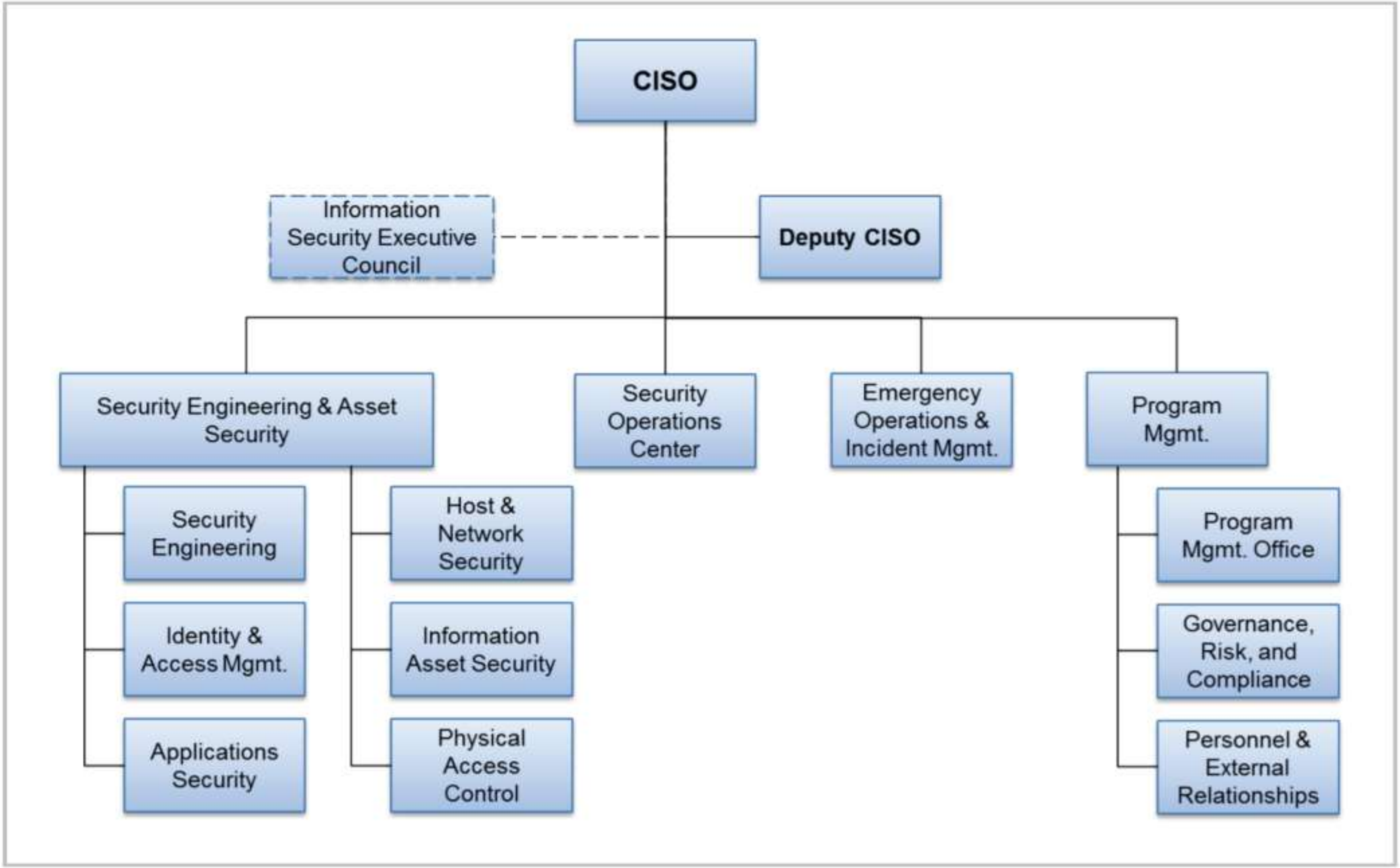

CISO
Information Security Executive Council
Deputy CISO
Security Engineering & Asset Security
Security Operations Center
Emergency Operations & Incident Mgmt.
Program Mgmt.
Security Engineering
Identity & Access Mgmt.
Applications Security
Host & Network Security
Information Asset Security
Physical Access Control
Program Mgmt. Office
Governance, Risk, and Compliance
Personnel & External Relationships

Figure 3: CISO Organizational Structure

Solutions

The Anna Karenina Principle

“Happy families are all alike; every unhappy family is unhappy in its own way.”

Regulatory Developments

- Gopalakrishna Committee report (Jan 2011)
  - Expertise at the Board level
  - Oversight and structures required for IT governance
  - Information Security Function, headed by the CISO, directly reporting to an Executive Director
  - Information Security Steering Committee, headed by the CEO/designated ED
  - Information Security Programme
- Cyber Security Circular (June 2016)
  - Board approved Cyber Security Policy
  - Arrangement for continuous monitoring (Security Operations Centre)
  - IT architecture should be conducive to security
  - Protecting customer information
  - Cyber Crisis Management Plan (CCMP)
  - Incident reporting and information sharing
  - Cyber security awareness, among employees, management and board

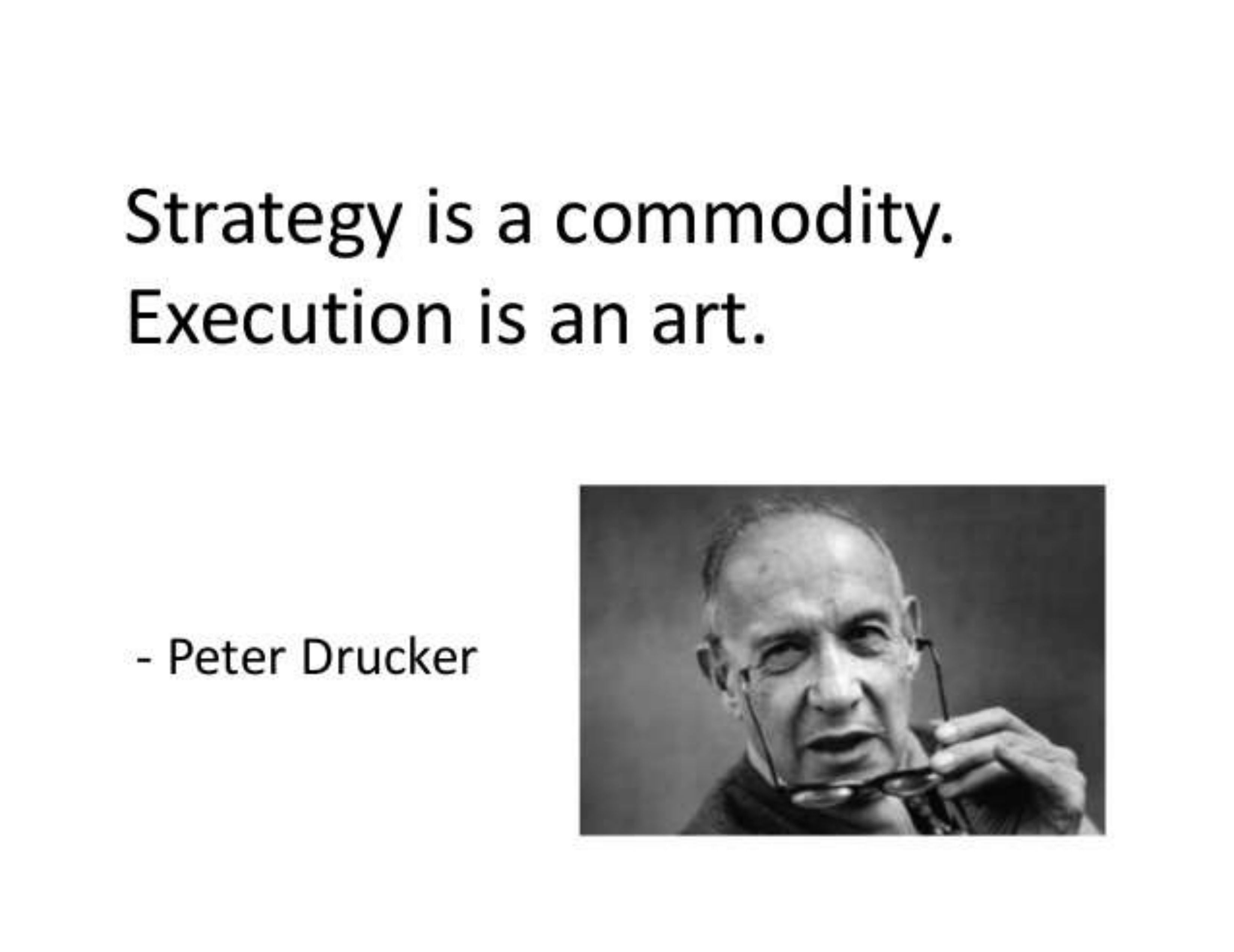
India: Cyber Security Infrastructure

- The law: Information Technology Act, 2000, amended in 2008
- The structure
  - Computer Emergency Response Team CERT-In/ CERT-Fin /Bank-CERT
  - National Critical Information Infrastructure Protection Centre (NCIIPC)
- The Programmes (five years or more)
  - Cyber Swachchhata Kendra
  - Maharashtra Cyber Project (Rs 800 crore)
  - National Cyber Coordination Centre (Rs 800 crore)
  - MHA Cyber and Information Security Division (Rs 400 crore)
  - Funding for developing indigenous security technology (Rs 1000 crore)
- Comparison
  - UK funding > 17K crore over five years
  - US federal spend annual ~ 1,78,000 crore

- What needs improvement
  - Privacy framework for enabling better data harvesting and usage
  - Customer grievance redressal mechanism
  - Inter-state Law Enforcement mechanism for cyber crime response
  - Forensic capabilities of organisations/police
  - Supply of cyber security skills

Recap

- The security scenario is getting worse, with larger data breaches routinely reported
- Focus shifting from Prevent/Detect to Respond/Recover
- Countermeasures require close collaboration among multiple teams, including LEA
- Confluence of physical/cyber threats
- India needs to invest significantly, to survive and to thrive



Strategy is a commodity.
Execution is an art.

- Peter Drucker