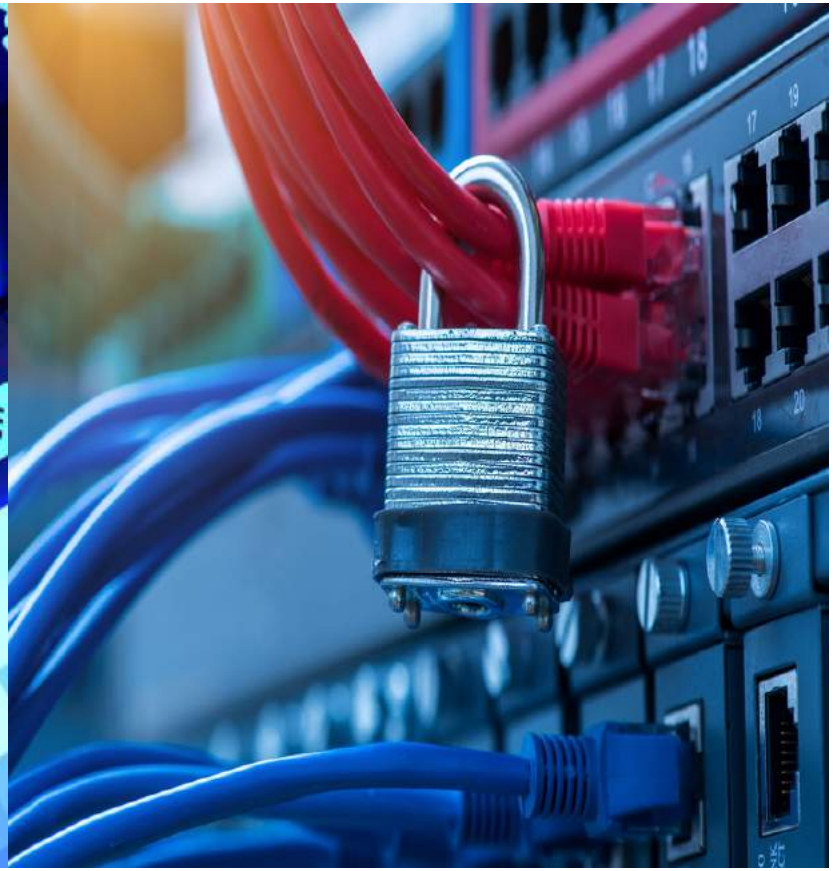


Cyber Security

by

Dr VK Saraswat

Member, NITI Aayog

Cyberspace

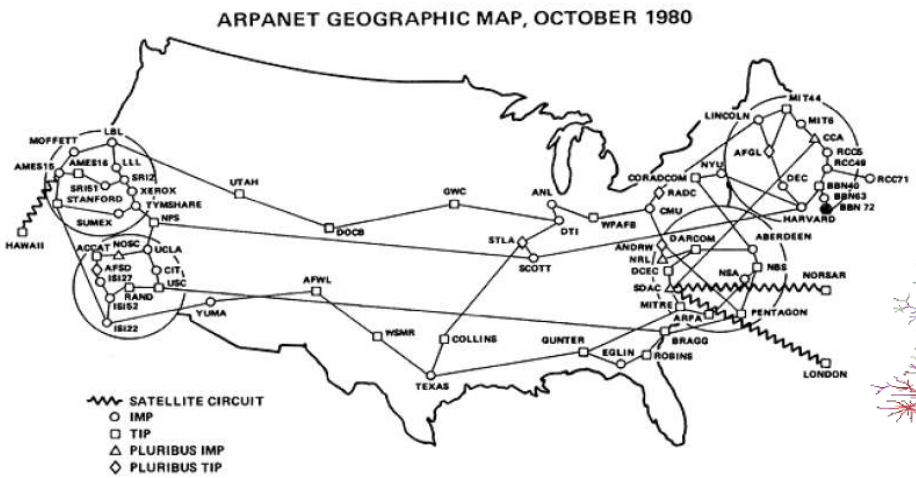
"A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

-- A Definition of Cyberspace

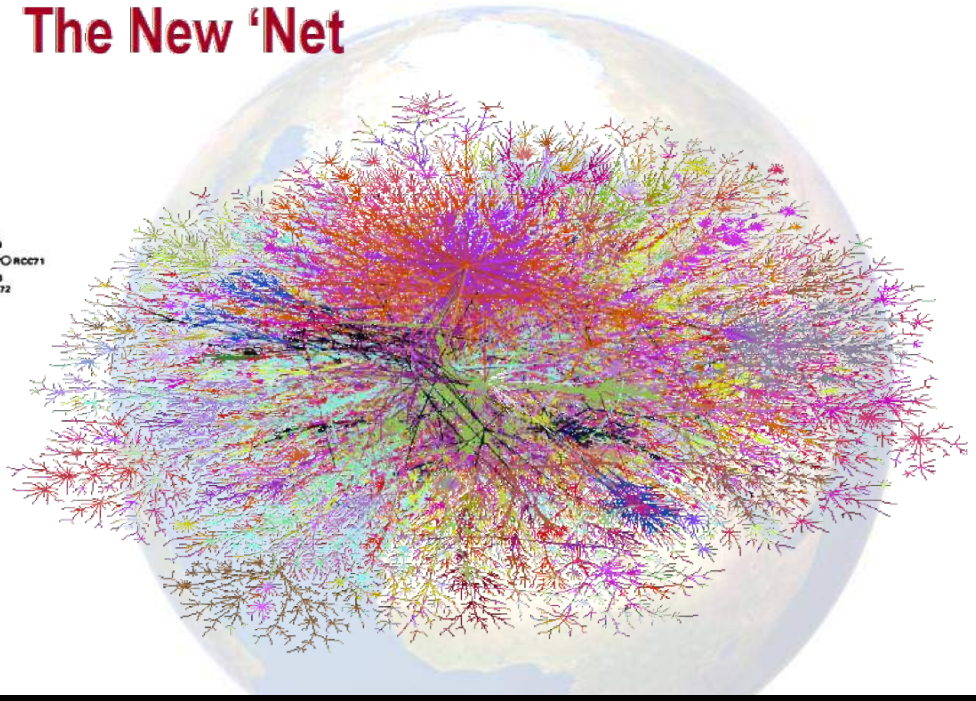
Life in a Networked World

- **Rapid Development in Information Technology**
  - Speed of Microprocessor chips doubles every 12-18 months
  - Storage Density doubles every 12 months
  - Bandwidth is doubling every 12 months
  - Price keeps dropping making technology affordable & pervasive

The Old 'Net



The New 'Net



The New "Net" monitors & controls critical Infrastructure. Its integrity & availability is critical for economy, public safety, & national security

The Internet In India by 2020

730
Million Internet Users

75%
New users from Rural Areas

75%
New users to consume data in vernacular languages

83%
CAGR mobile video content growth

175
Million on-line shoppers

70%
E-commerce transactions will be via mobile

50%
Travel transactions will be online

Indian Economy Marching the e-way

Cyber What? Defining Cyber

- Cyberspace is the connected Internet Ecosystem

- Trends Exposing critical infrastructure to increased risk:
  - Interconnectedness of Sectors
  - Proliferation of exposure points
  - Concentration of Assets

- Cyber Intrusions and Attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy

- Cyber Security is protecting our cyber space (critical infrastructure) from attack, damage, misuse and economic espionage

Cyber Security Challenges

- Cyberspace has inherent vulnerabilities that cannot be removed
- Innumerable entry points to internet.
- Assigning attribution: Internet technology makes it relatively easy to misdirect attribution to other parties
- Computer Network Defense techniques, tactics and practices largely protect individual systems and networks rather than critical operations (missions)
- Attack technology outpacing defense technology
- Nation states, non-state actors, and individuals are at a peer level, all capable of waging attacks

Evolution Of Cyber Security

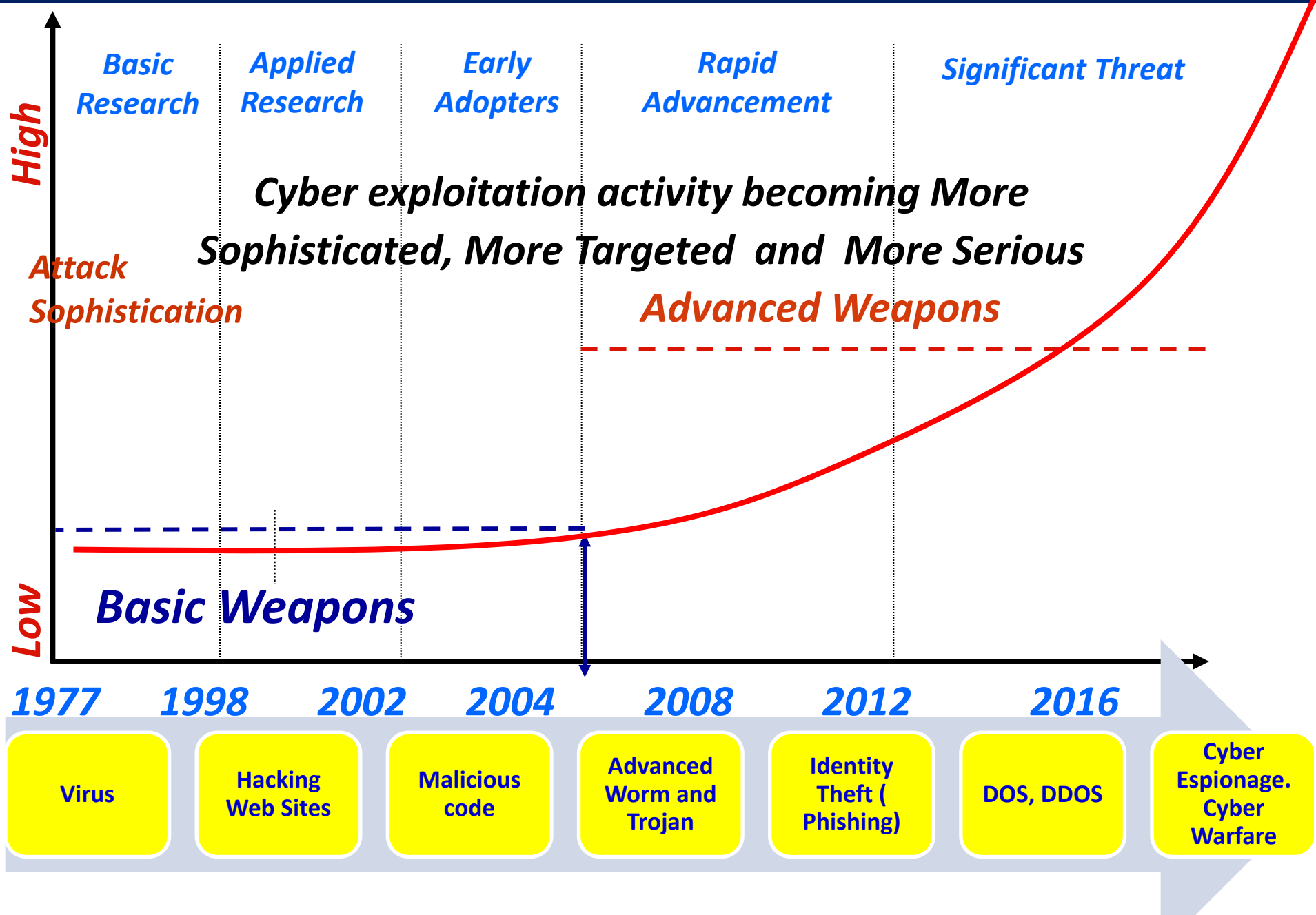
Viruses (1990s)
Anti-Virus, Firewalls

Worms (2000s)
Intrusion Detection & Prevention

Botnets (late 2000s to Current)
DLP, Application-aware Firewalls, SIM

APT, Insiders (Current)
Network Flow Analysis

Cyber Threat Evolution



Indian Cyber Situation

- India ranks 3rd in terms of the highest number of internet users in the world after USA and China, the number has grown 6-fold between 2012-2017 with a compound annual growth rate of 44%.

- India secures a spot amongst the top 10 spam-sending countries in the world alongside USA

- India was ranked among the top five countries to be affected by cybercrime, according to a 22 October report by online security firm ”Symantec Corp”.

Cyberattacks in India of Late

JULY 2016

UNION BANK OF INDIA HEIST

Through a phishing email sent to an employee, hackers accessed the credentials to execute a fund transfer, swindling Union Bank of India of $171 million, Prompt action helped the bank recover almost the entire money

MAY 2017

WANNACRY RANSOMWARE

The global ransomware attack took its toll in India with several thousands computers getting locked down by ransom-seeking hackers. The attack also impacted systems belonging to the Andhra Pradesh police and state utilities of West Bengal

MAY 2017

DATA THEFT AT ZOMATO

The food tech company discovered that data, including names, email IDs and hashed passwords, of 17 million users was stolen by an 'ethical' hacker-who demanded the company must acknowledge its security vulnerabilities-and put up for sale on the Dark Web

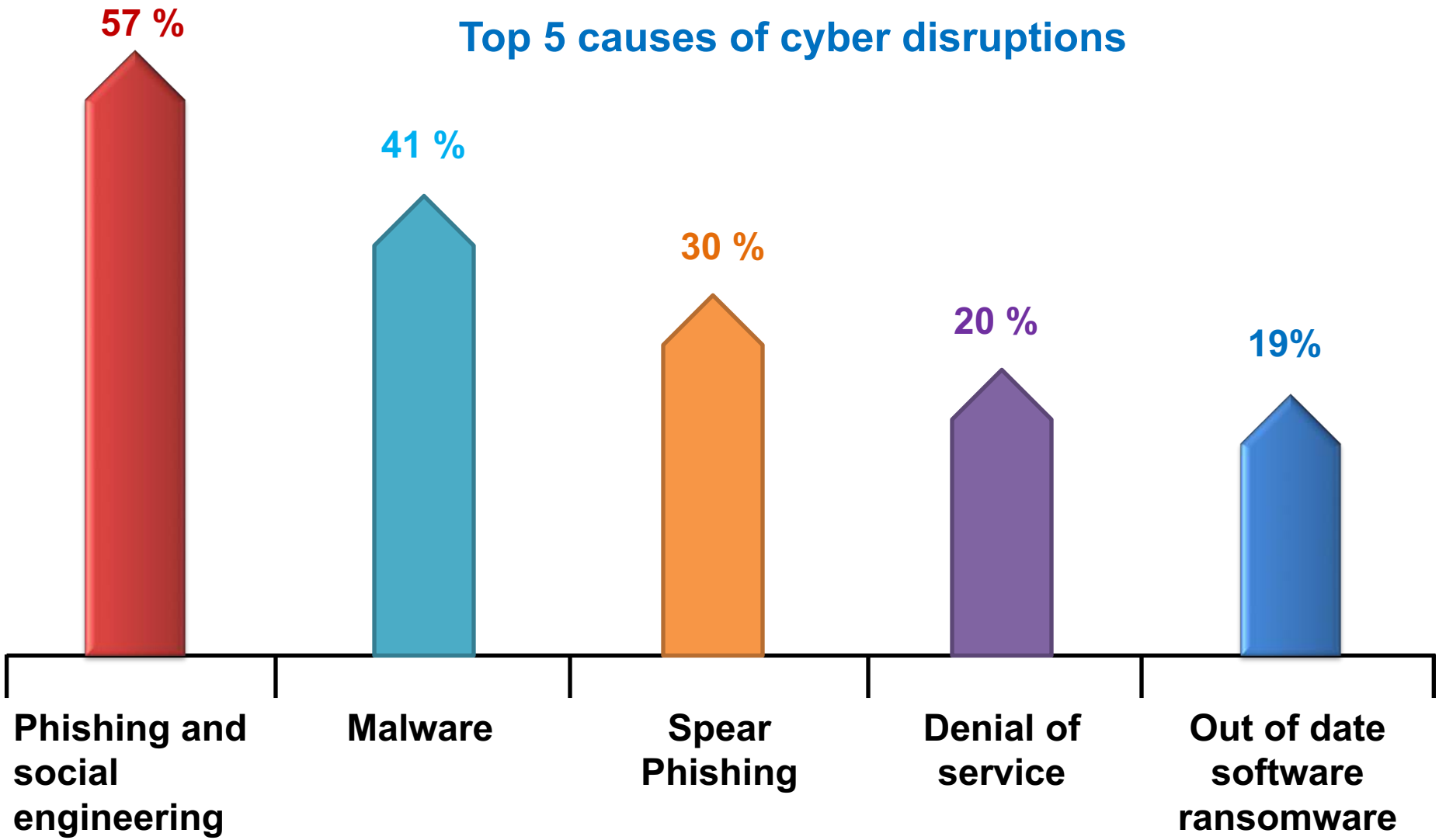
JUNE 2017

PETYA RANSOMWARE

The ransomware attack made its impact felt across the world, including India, where container handling functions at a terminal operated by the Danish firm AP Moller-Maersk at Mumbai's Jawaharlal Nehru Port Trust got affected

Cyber disruptions

> 50 % of the organization s reportedly affected in 2017

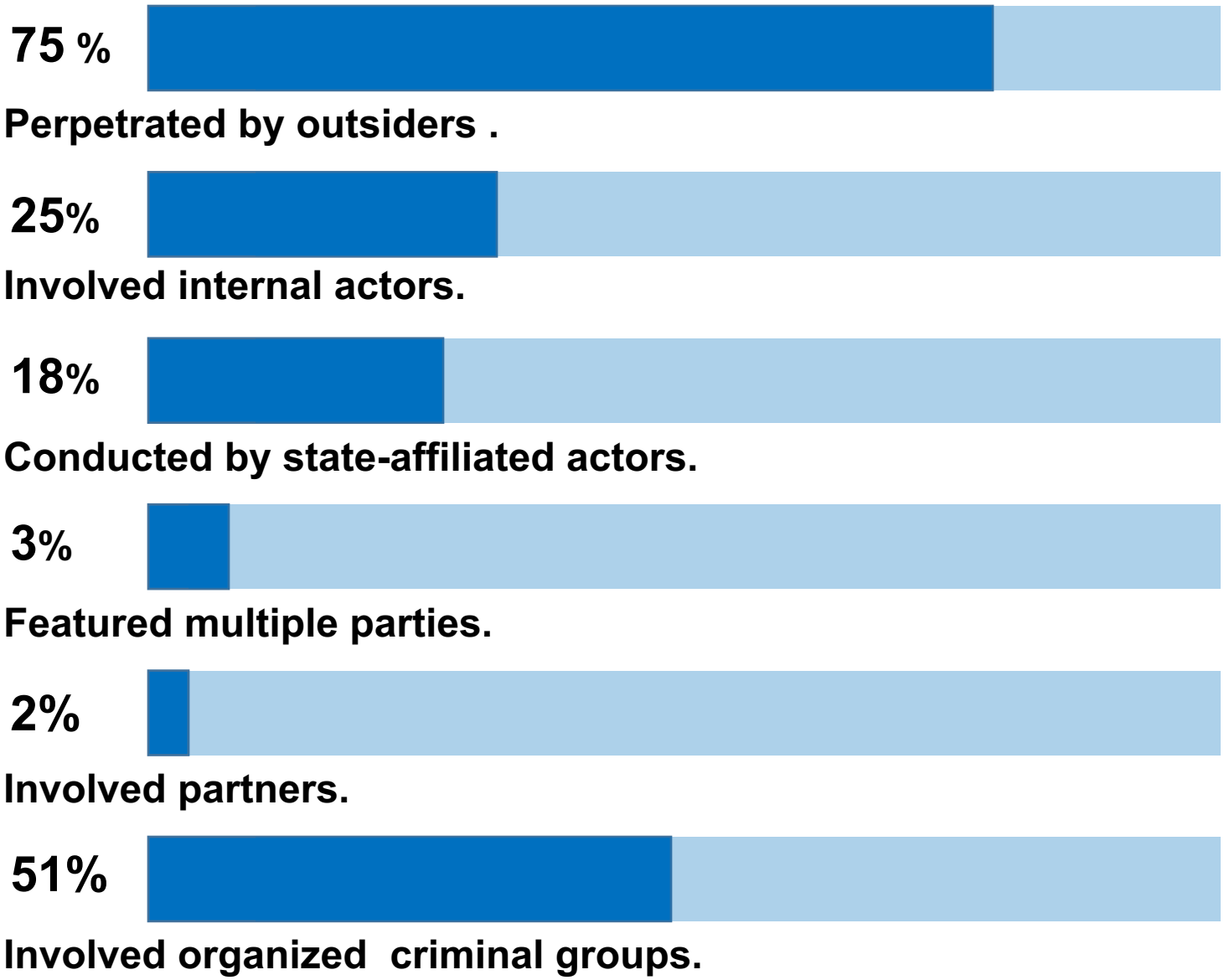


Financial and Insurance

Frequency	998 incidents, 471 with confirmed data disclosure
Top 3 patterns	1. Denial of Services, 2. Web Application Attacks and 3. Payment Card skimming Represent 88 % of all security incidents within financial services
Threat actors	94% External, 6 % Internal, <1% Partner (all incidents)
Actor Motives	96% Financials, 1% Espionage (all incidents)
Data Compromised	71% Credentials, 12 % Payment, 9% Personal
Summary	DoS attacks were the most common incident type. Confirmed data breaches were often associated with banking Trojans stealing and reusing customer passwords, along with ATM skimming operations

Source: 2017 Data Breach Investigations Report (DBIR) - Verizon

Who's behind the breaches?



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%

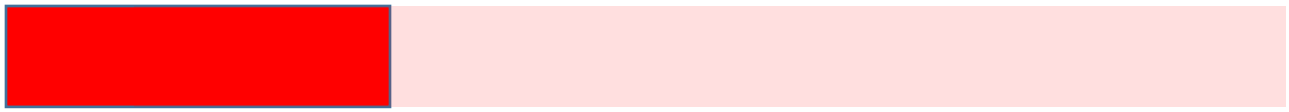
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8%

Physical actions were present in 8% of breaches

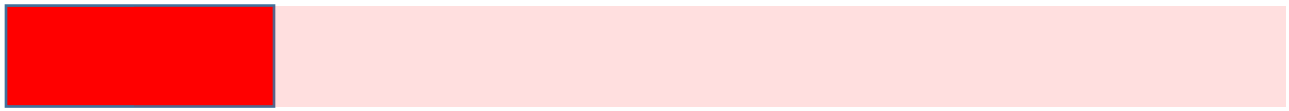
Who are the victims?

24 %



of breaches affected financial organizations.

15%

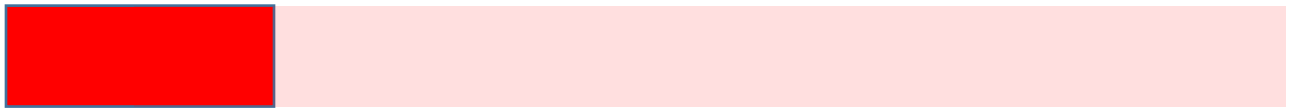


of breaches involved healthcare organizations.

12%

Public sector entities were the third most prevalent breach victim at 12%

15%



Retail and Accommodation combined to account for 15% of breaches.

What else is common?

66 %

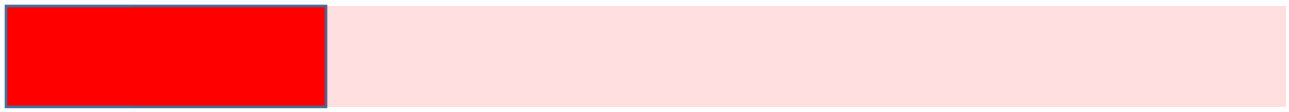
of malware was installed via malicious email attachments.

73%

of breaches were financially motivated.

21%

of breaches were related to espionage



27%

of breaches were discovered by third parties.

International Security Trends

Cyber criminals steal personal data to affect the operations of e-commerce and finance

Organized hackers use Advanced Persistent Threat (APT) attacks to steal the confidential data of official, national defense and business

The open systems and the Internet are used in critical infrastructures increasingly. That results in the growing of the risks.

Information and security providers have been hacked to lead to damage the trusted supply chain

Cyber-warfare and DDoS paralyzed national network operations

THE BIGGEST CYBER ATTACKS

TOI

Credits: Getty Images/iStockphoto

CryptoLocker (2013)

Infected more than **2,50,000 systems**

Earning **$3 mn**

CryptoWall (2014-16)

Extorted **$18 million** from victims prompting FBI to release an advisory

TeslaCrypt (2015)

Hit **163** victims netting **$76,522** for attackers

WannaCry (2017)

Hit **2,00,000+ systems**

VULNERABLE TO RISKS

75%

of Indian CXOs admit they lack confidence in their companies' cybersecurity processes

26%

Share of respondents whose security operations centres collaborate and share data with others in the industry

69%

of respondents say their budgets to combat cyber threats increased over the past 12 months

CXOs surveyed: 124

Source: *EY Global Information Security Survey 2016-17—India Report*

RANSOMWARE STATISTICS 2017

Cybercrime damages will cost the world **$6** trillion annually by 2021

156 million phishing emails are sent globally everyday

91% of Cyberattacks start with a phishing email

In 2017, **1 in 131** emails contained Malware

According to FBI, more than **4000** ransomware attacks occur daily

Ransomware attacks increased by **36%** in 2017

In 2017, every 4.2 seconds, a new malware specimen emerged (according to GData)

24BY7 SECURITY

Cybersecurity and Compliance Specialists

www.24by7security.com

Cyber Threats and Sources

Sources

a) Nation States
b) Cyber Criminal Organisations
c) Terrorists, DTOs, etc.,
d) Hackers / Hacktivists

Threats

- Malware – Malicious software to disrupt computers
- Viruses, worms, …
- Theft of Intellectual Property or Data
- Hactivism – Cyber protests that are socially or politically motivated
- Mobile Devices and applications and their associated Cyber Attacks
- Social Engineering – Entice Users to click on malicious links
- Spear Phishing – Deceptive Communications (e-mails, texts, tweets)
- Domain Name System (DNS) Attacks
- Router Security – Border Gateway Protocol (BGP) Hijacking
- Denial of Service (DoS) – blocking access to websites
- Others
- **Bottom line – easier to be a Bad Guy and volume of threats is growing**

Main *Cyber* Players and their Motives

- ***Cyber Criminals:*** Seeking commercial gain from hacking banks & financial institutions as well a phishing scams & computer ransom ware
- ***Cyber Terrorists:*** Mission to penetrate & attack critical assets, and national infrastructure for aims relating to political power & "branding"
- ***Cyber Espionage:*** Using stealthy IT Malware to penetrate both corporate & military data servers in order to obtain plans & intelligence
- ***Cyber Hackivists:*** Groups such as "Anonymous" with Political Agendas that hack sites & servers to virally communicate the "message" for specific campaigns

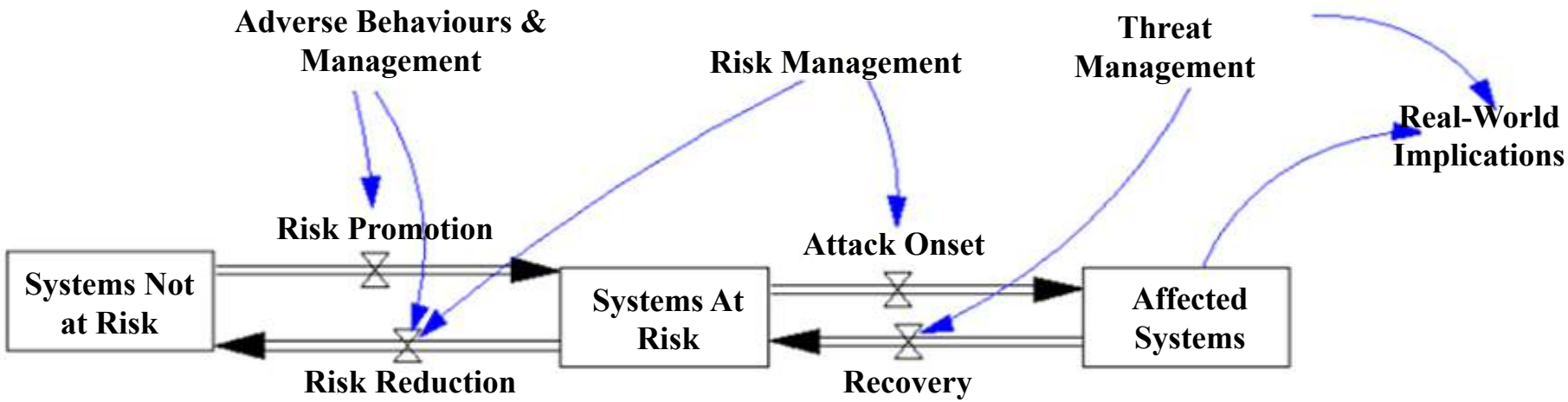
Dynamics of Threats and Resilience
(using System Dynamics modeling)

How did breaches (threats) occur?*

67% were aided by significant errors (of the victim)

64% resulted from hacking

38% utilized Malware



How are security and threat processes (resilience) managed? *

Over 80% of the breaches had patches available for more than 1 year

75% of cases go undiscovered or uncontained for weeks or months

Real World System

Correctly conveying intent & receiving result

Correct processing of user intent

Correct execution of Compute algorithms

Correct execution environment

HMI

Compute Algorithms

SW Architecture

Authentication

Crypto Algorithms
Security Protocols

Resource Alloc
Process Isolation

Key Storage
Compute Logic

- Upper Layer can depend on lower layer only if it has higher
  - Integrity
  - Availability
- Software builds on hardware
- Hardware is the *root* of trust

Security begins with a *trustworthy* hardware!!!

Hardware Cyber Security Concerns (1/2)

- Most equipment and technology for setting up Cyber Security infrastructure in India are currently procured from global sources. These systems are vulnerable to cyber threats just like any other connected system.

- There are various types of hardware attacks which includes the following.

  - Manufacturing backdoors may be created for malware or other penetrative purposes. Backdoors may be embedded in radio-frequency identification (RFID) chips and memories.

  - Unauthorized access of protected memory

  - Inclusion of faults for causing the interruption in the normal behavior of the equipment.

  - Hardware tampering by performing various invasive operations

  - Through insertion of hidden methods, the normal authentication mechanism of the systems may be bypassed.

Hardware Cyber Security Concerns (2/2)

- Above hardware attacks may pertain to various devices or systems like:
  - Network systems
  - Authentication tokens and systems
  - Banking systems
  - Surveillance systems
  - Industrial control systems
  - Communication infrastructure devices

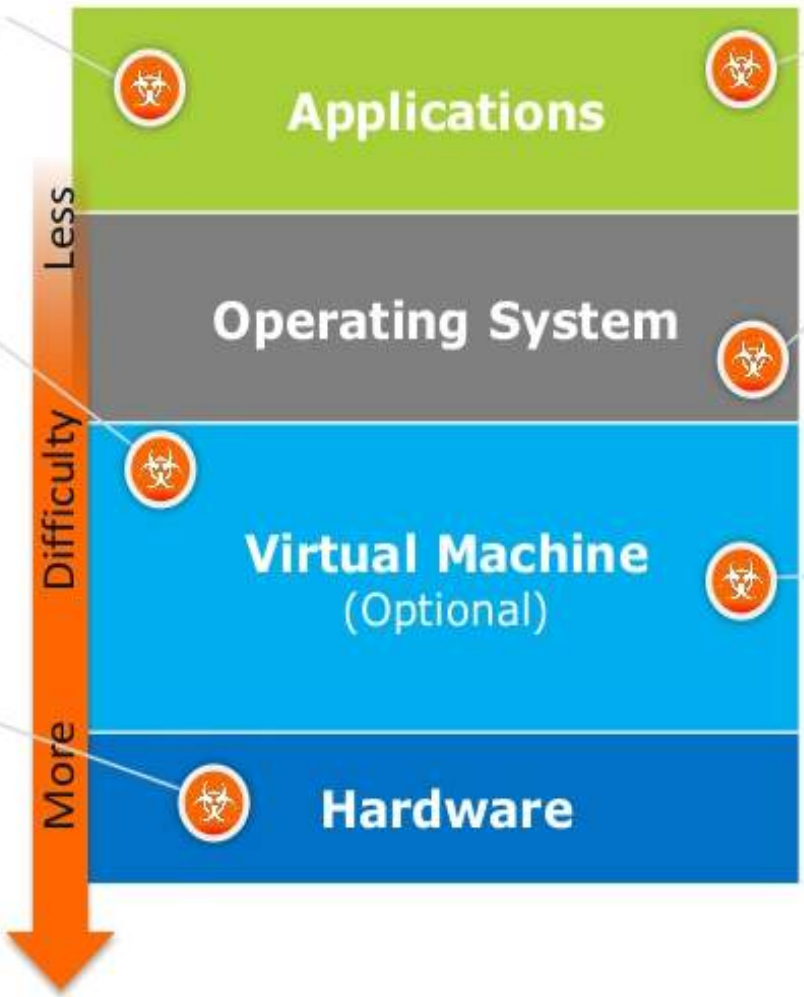
Innovations to Attack: End-Points Example

Attackers are adapting by moving down the stack:

Attacks disable security products, steal and control applications

Compromise virtual machine

Attacks against hardware and firmware affect the root-of-trust

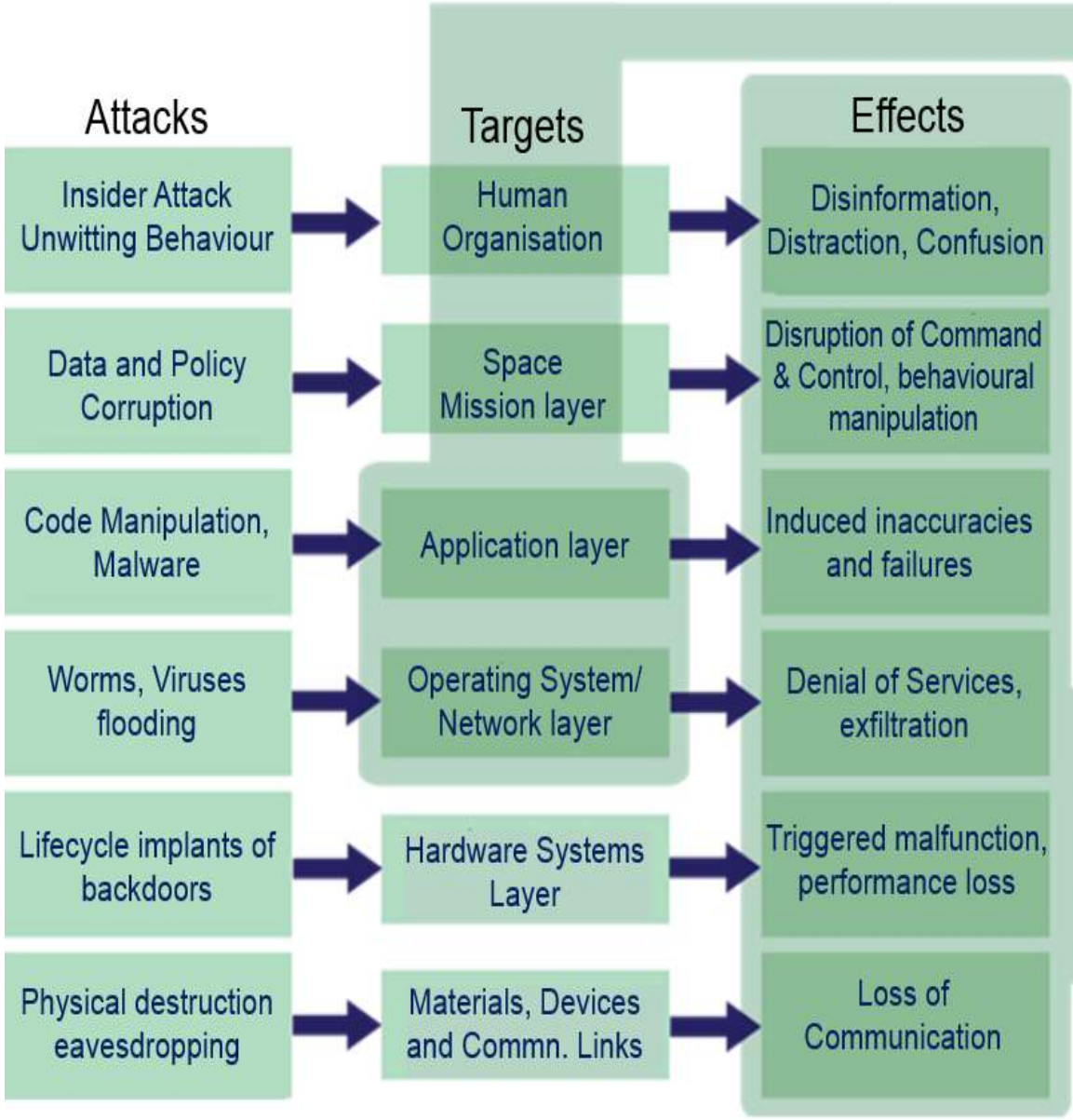


Traditional attacks: Focused primarily on the application layer

OS infected: Threats are hidden from security products

New stealth attacks: Embed themselves below the OS and Virtual Machine, so they can evade current solutions

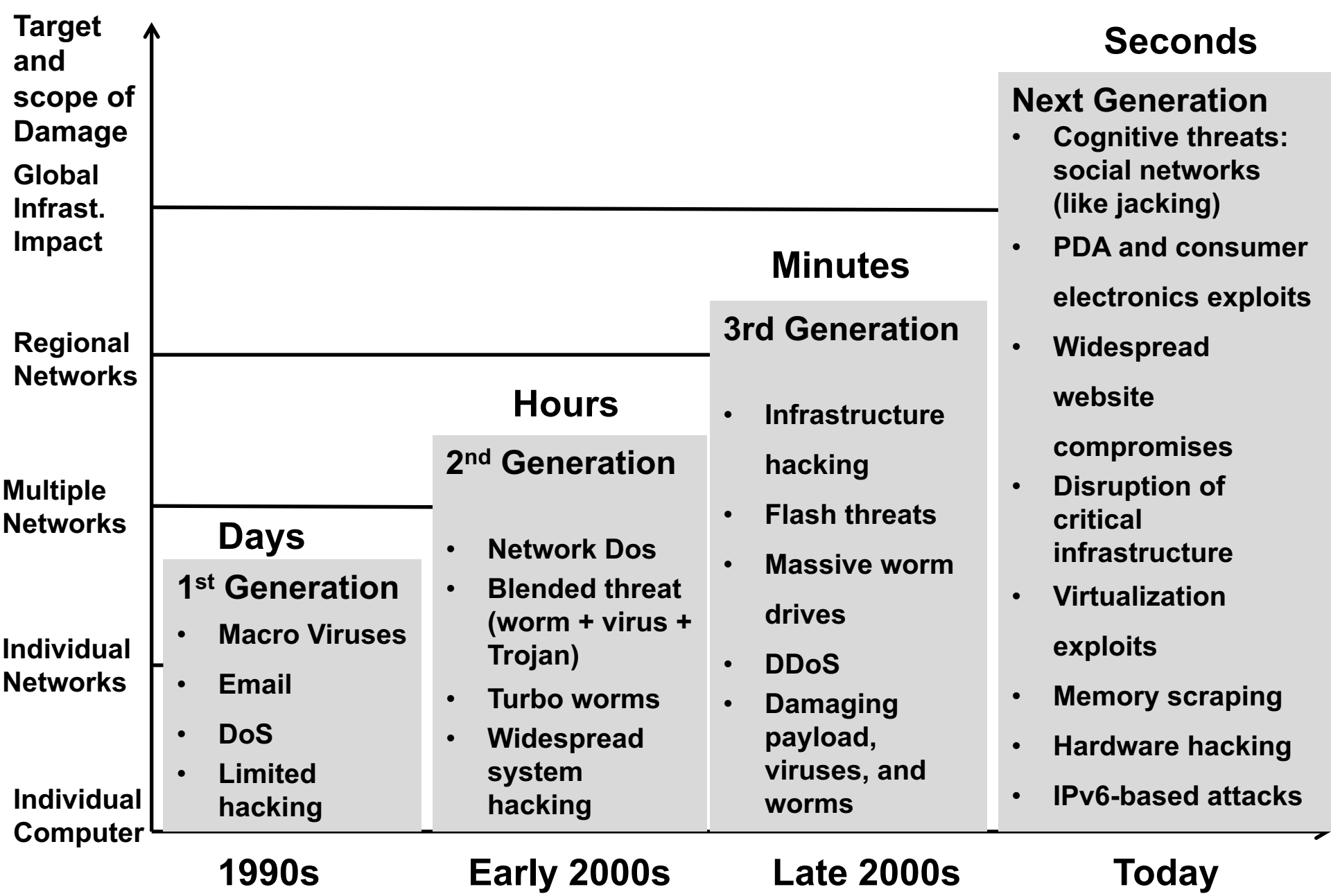
Challenges are increasing in the Cyber Space Domain



- Net-centricity and interoperability increase the risk of cyber-attacks
- Software is the most apparent target of cyber-attacks, especially when plagued with a lack of quality, questionable pedigree and uncontrolled access to development environments

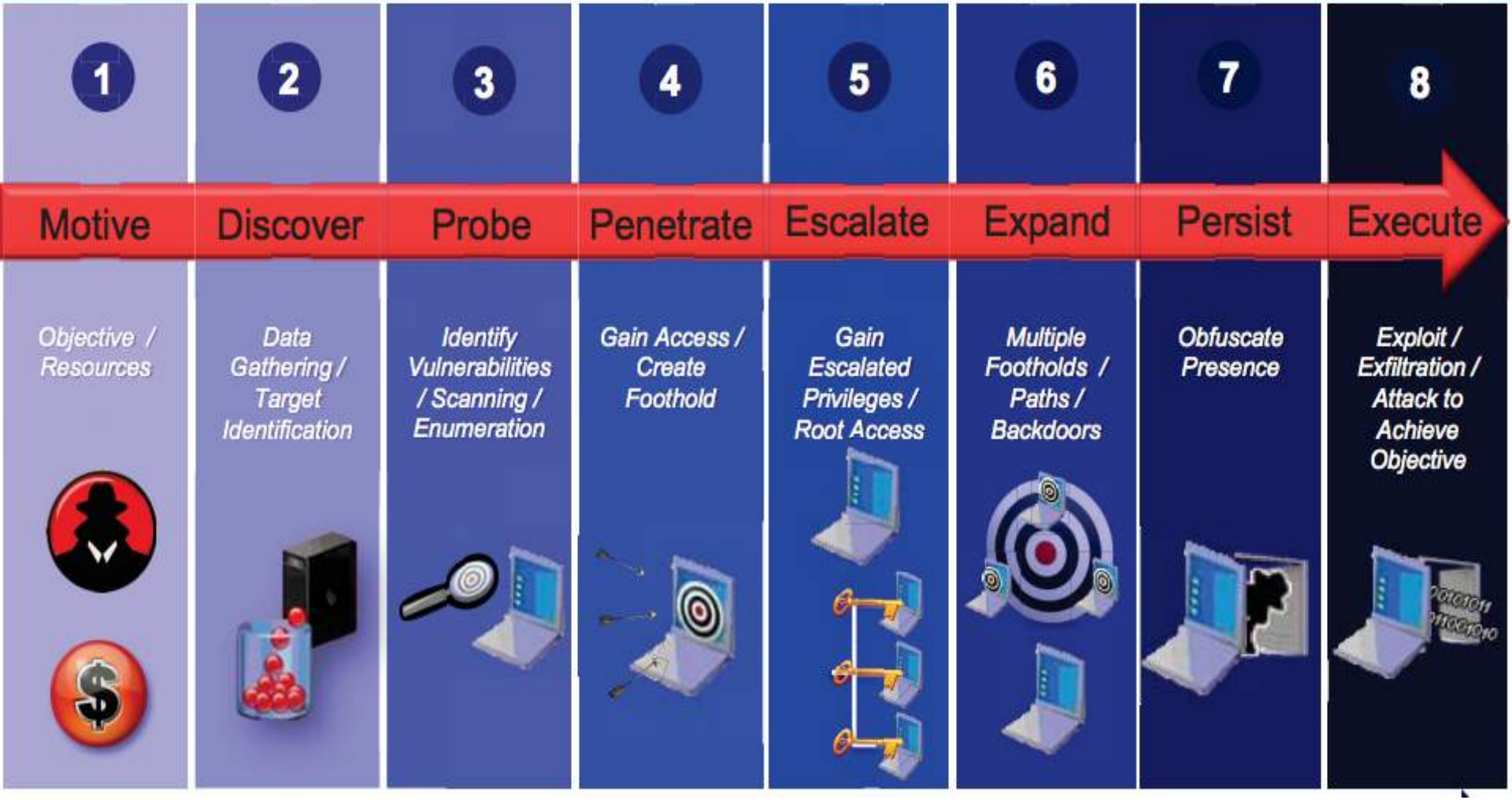
Mitigation is a challenge – it requires:

- Development Environment access control
- Architectural considerations
- Technology and tools
- Informed operator responsiveness



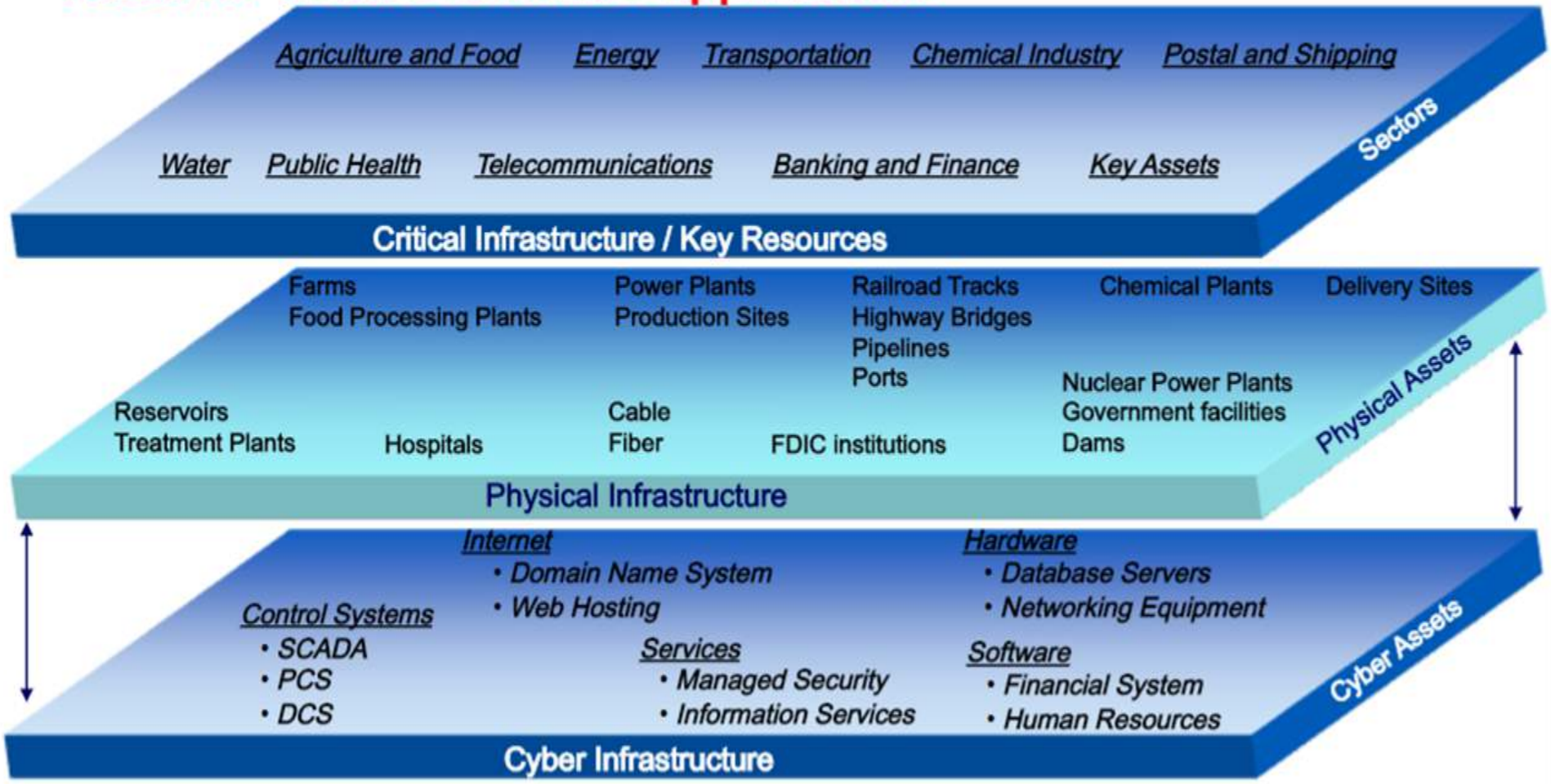
Shrinking Time Frame from Knowledge of Vulnerability to Release of Exploits

Anatomy of Attack



Cyberspace & physical space are increasingly intertwined and software controlled/enabled

Need for secure software applications



"In an era riddled with asymmetric cyber attacks, claims about system reliability, integrity and safety must also include provisions for built-in security of the enabling software."

Cyber security

Information Security and Cryptography Technologies

System Security Technology

- Protecting Peripheral Components
- Protecting Distributed Contents
- Trusted Computing Platforms
- Detecting Intrusion/ Malware
- Protecting Data/Access Control
- Authentication

Network Security Technology

- Protecting Privacy or Anonymity
- IEEE 802.11
- Security Pairing

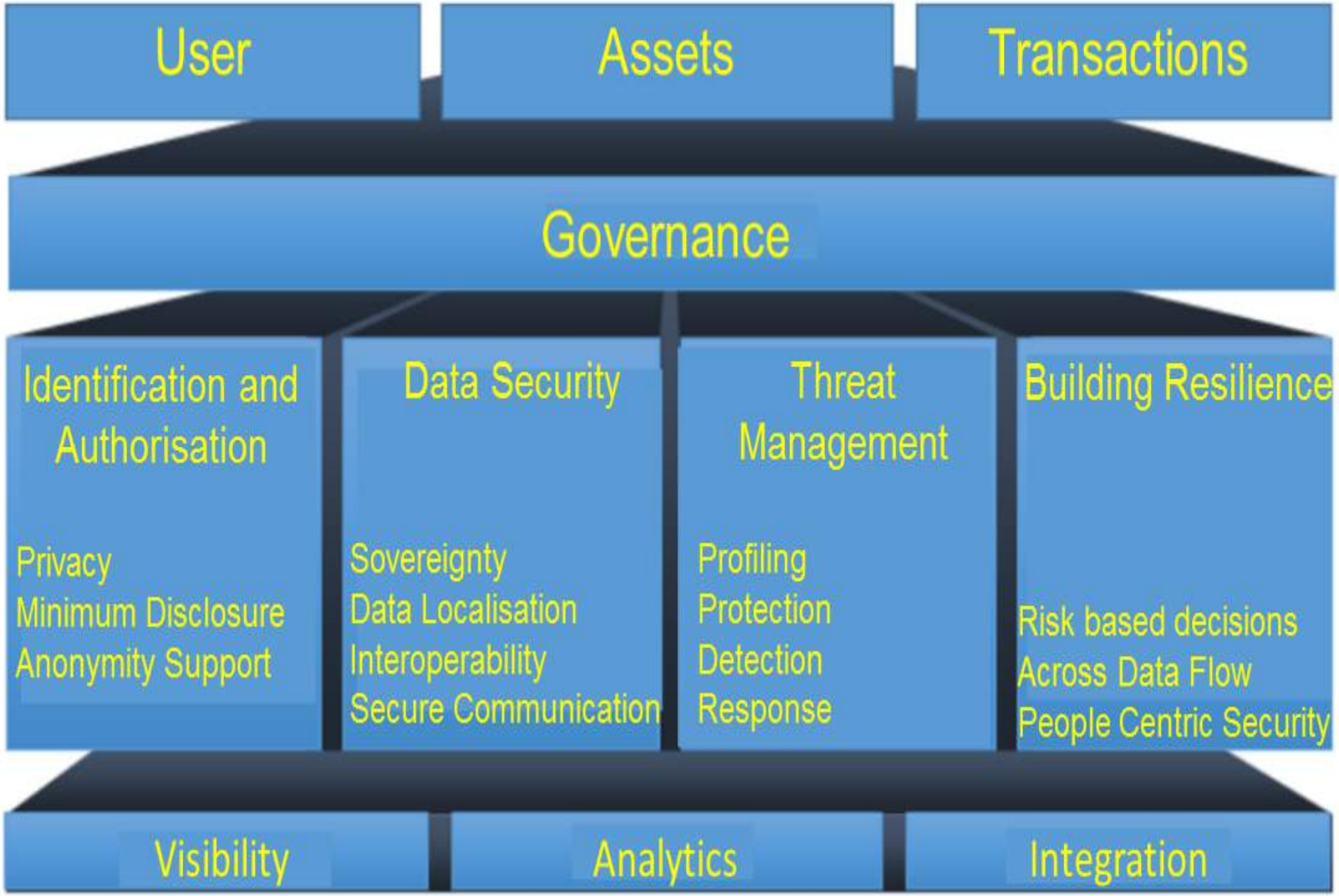
Wireless Network Security Technology

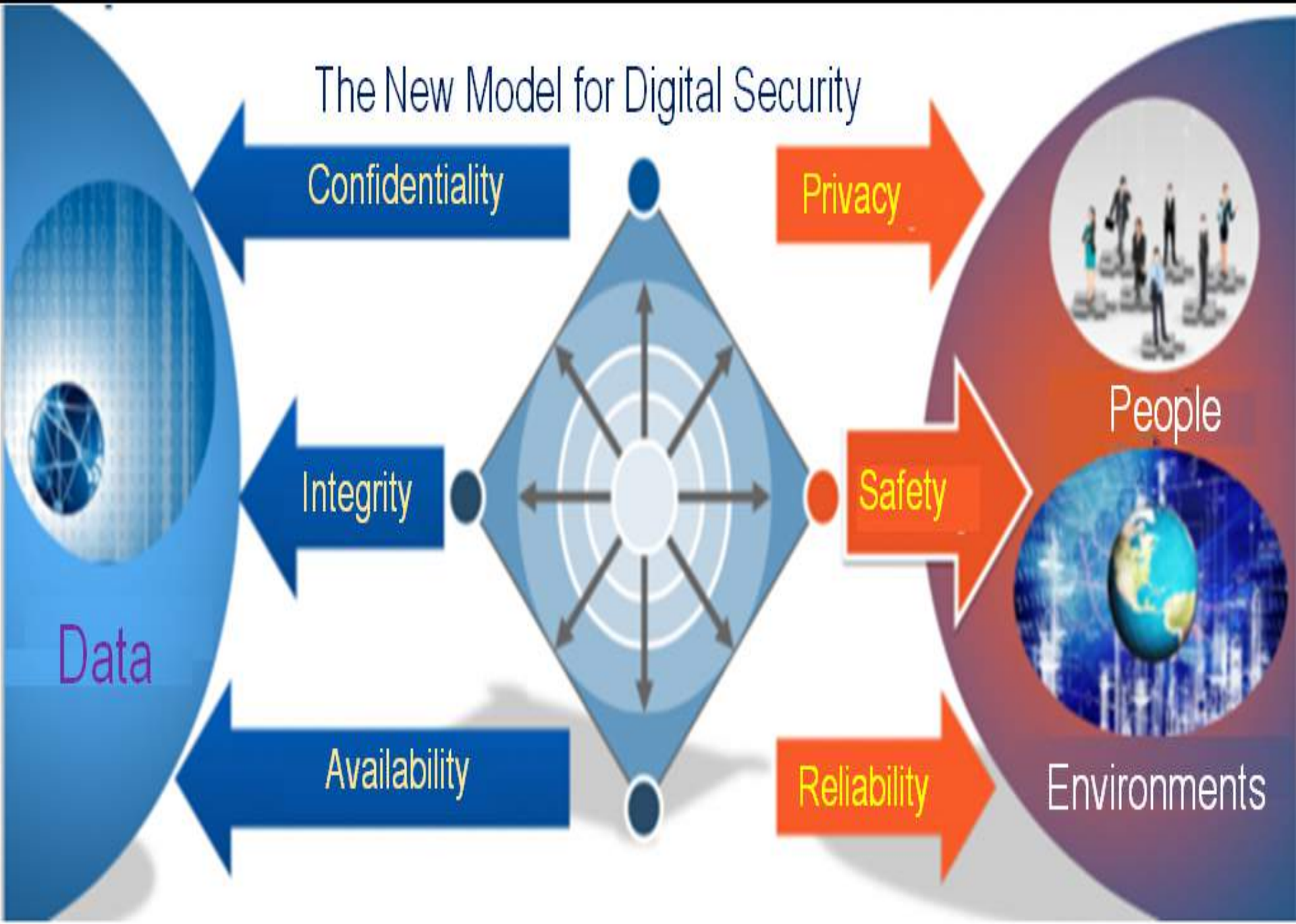
- Security at particular protocol layers
- Detecting Malicious traffic
- Key Management

Cryptography

- Symmetric Cypher
- Asymmetric Cypher
- PKI-Digital certificate
- Secure hashing
- Key Management
- Quantum Cryptography

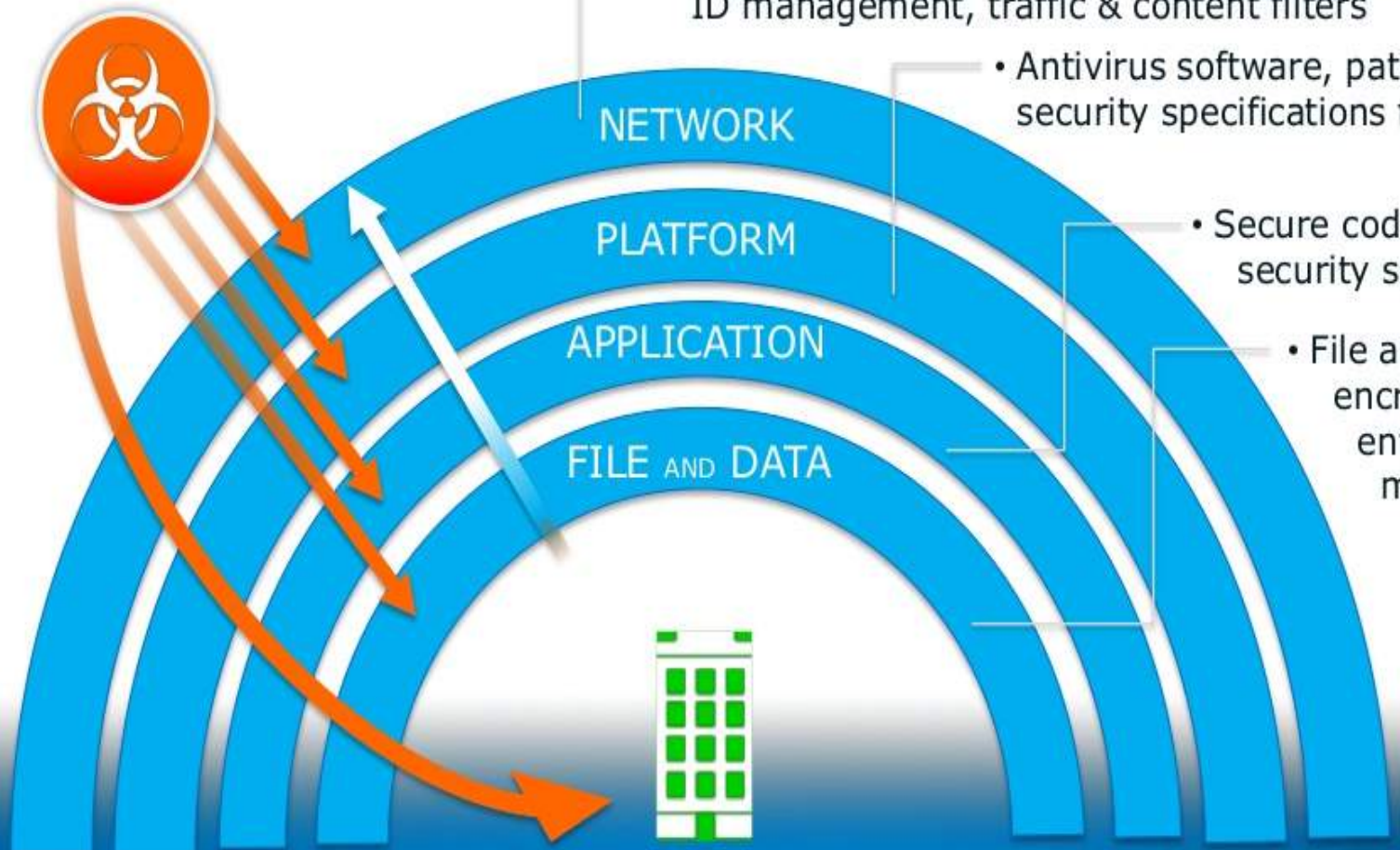
Cyber Security Framework




The New Model for Digital Security
Confidentiality
Integrity
Availability
Privacy
Safety
Reliability
Data
People
Environments

Tactical Security Technology Integration: Layered Defense

Multiple layers are necessary for comprehensiveness



- Firewalls, demilitarized zones, data loss prevention, ID management, traffic & content filters
- Antivirus software, patching, minimum security specifications for systems
- Secure coding, testing, security specifications
- File and data encryption, enterprise rights management

IoT Cyber Security - Vulnerabilities

Operational Security

IOT Bases services require continuity and high availability

Privacy

Valuable Data Require Protection

Software Patching

Many IoT devices lack human users who can install security updates

Identity of Things

In the absence of universal standards, each implementation requires unique approach to manage authentication and access

Logging

Logging System must identify events without relying time of day data

Future Technology to be Designed with Security

Security must be part of the design for future technology. Adding security after, is no longer sufficient or sustainable

Smart

Security innovation must deliver more capable solutions to keep pace with threats

Open

Platforms and security standards must be open to promote collaboration and accelerate adoption

Trusted

Technology and security providers must be trustworthy in the creation and operation of their products

Strong

Products and services must be hardened to resist compromise and make security transparent to users

Ubiquitous

Security must protect data wherever it exists or is used, for all parties and devices across the compute landscape

Strategic Leadership: Defense in Depth

A strong process strategy will enable operational flexibility, while driving cost efficiency, and effectiveness

Defense in Depth
Cyber Security Strategy

Prediction

Predict the most likely attacks, targets, and methods

Proactive measures to identify attackers, their objectives and methods prior to materialization of viable attacks.

Prevention

Prevent or deter attacks so no loss is experienced

Secure the computing environment with current tools, patches, updates, and best-known methods in a timely manner. Educating and reinforcing good user behaviors.

Detection

Identify attacks not prevented to allow for rapid and thorough response

Efficient management of efforts to contain, repair, and recover as needed, returning the environment to normal operations

Response

Rapidly address incidents to minimize losses and return to a normal state

Monitor key areas and activities for attacks which evade prevention. Identifies issues, breaches, and attacks

10 Steps to Cyber Security (1/5)

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security. CESG recommend you review this regime – together with the nine associated security area described below – in order to protect your business against the majority of cyber threats

1. Network Security

Protect your networks against external and internal attack. Manage the network primer. Filter out unauthorised access and malicious contents. Monitor and test security controls

2. Malware Protection

Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the Orgn.

10 Steps to Cyber Security (2/5)

3. Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT system and networks. Analyse logs for unusual activity that could indicate an attack.

4. Incident Management

Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

10 Steps to Cyber Security (3/5)

5. User Education and Awareness

Produce user policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

6. Home and Mobile Working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline to all devices. Protect data both in transit and at rest

10 Steps to Cyber Security (4/5)

7. Secure Configuration

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory & define a base line build for all ICT devices.

8. Removable Media Controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before imported on the corporate system.

10 Steps to Cyber Security (5/5)

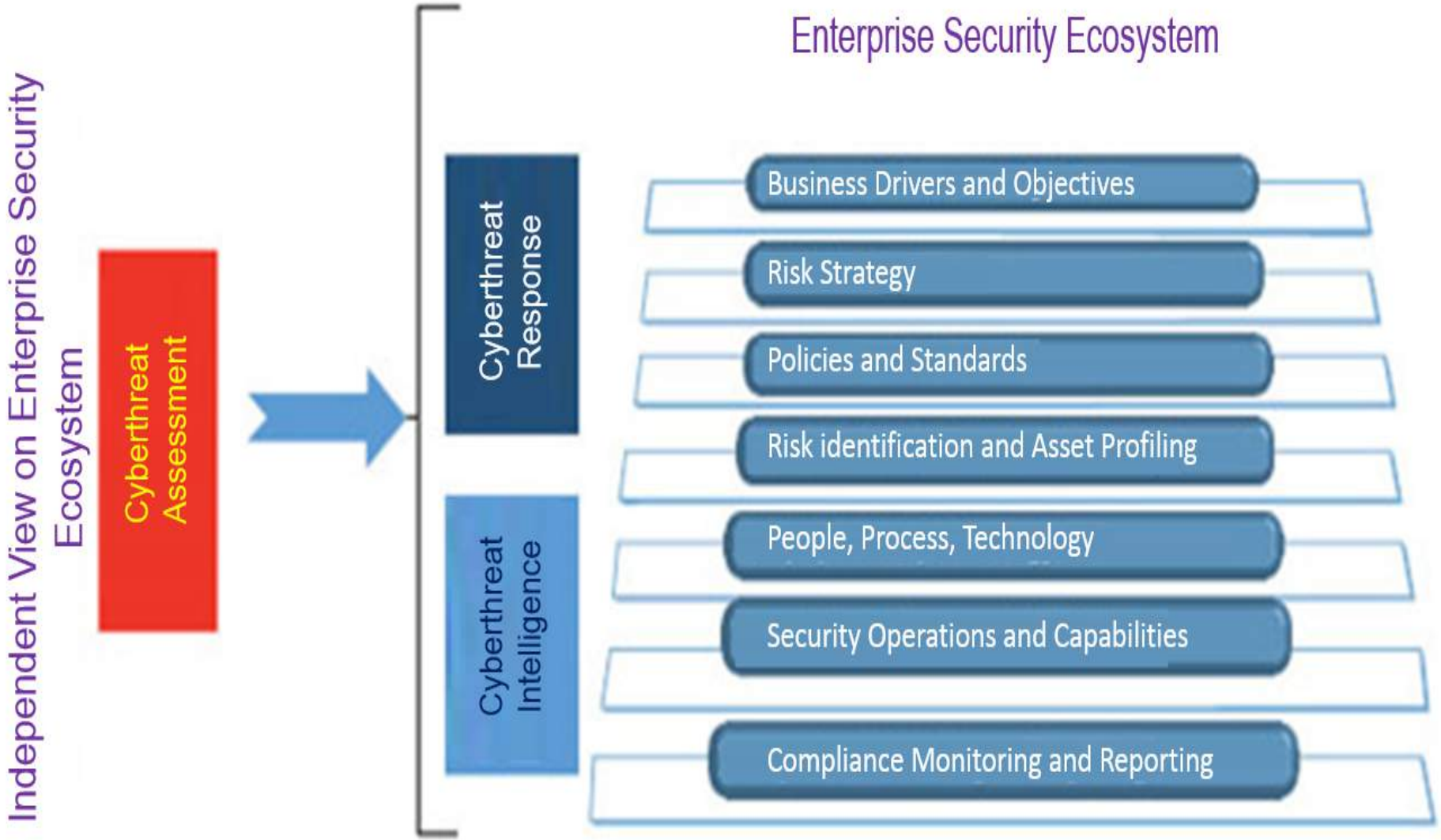
9. Managing User Privileges

Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

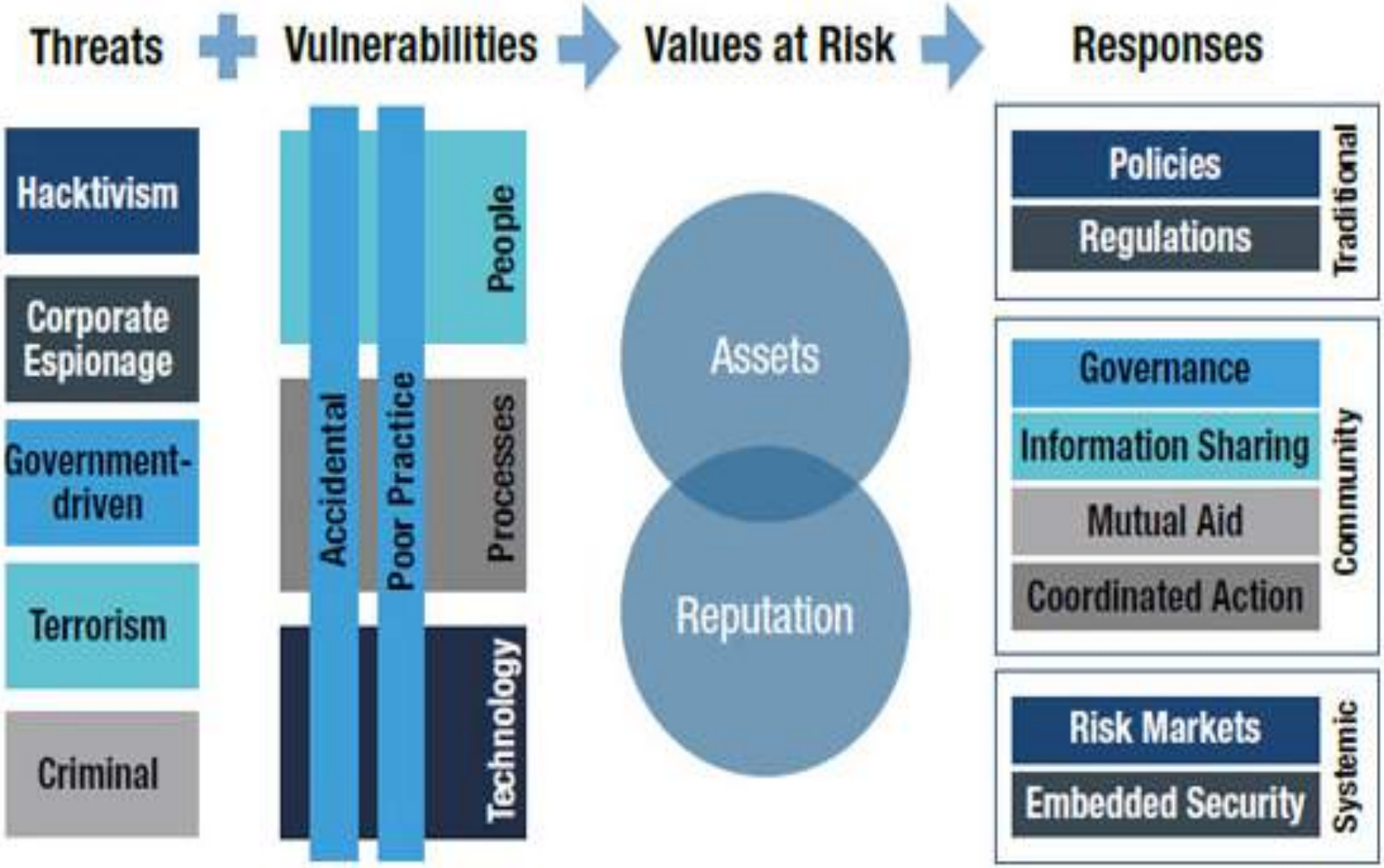
10 Information Risk Management Regime

Establish and effective governance structure and determine your risk appetite. Maintain boards engagement with cyber risk. Produce supporting information risk management policies.

Evolution of Cyberthreat Management



World Economic Forum Cyber Risk Framework

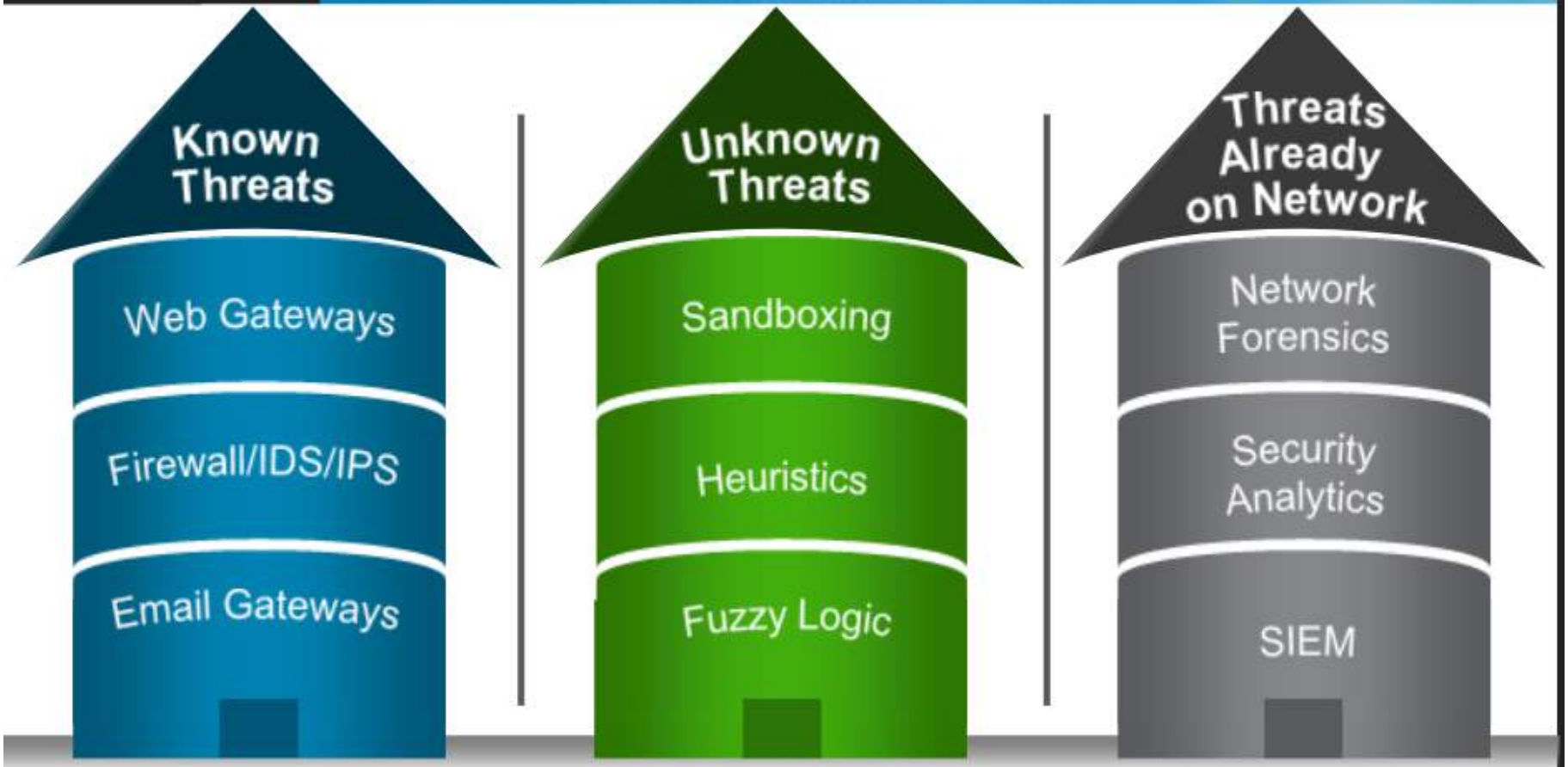


Cyber Security Planning

Cyber Trust Layer (1)	Organization heads meet and discuss the criteria for their mutual cyber trust. Network vulnerabilities will be ranked by this criteria
Cyber Impact Layer (2)	Organization heads meet and discuss how their mutually agreed upon criteria will affect their cyber risk. The result drives criteria weights.
Cyber Analytic Layer (3)	Cyber security researchers develop a set of custom scientific metrics to assess the Global Severity of identified network vulnerabilities which are ranked by the agreed upon criteria
Cyber Metric Implementation Layer (4)	Cyber security researchers meet with network engineers to develop continuous monitoring framework to identify vulnerabilities and to calculate metrics.
Cyber Evaluation Layer (5)	Organization heads meet to discuss their individual Cyber Maturity and to determine the minimum risk-level necessary for collaboration

BLUE COAT

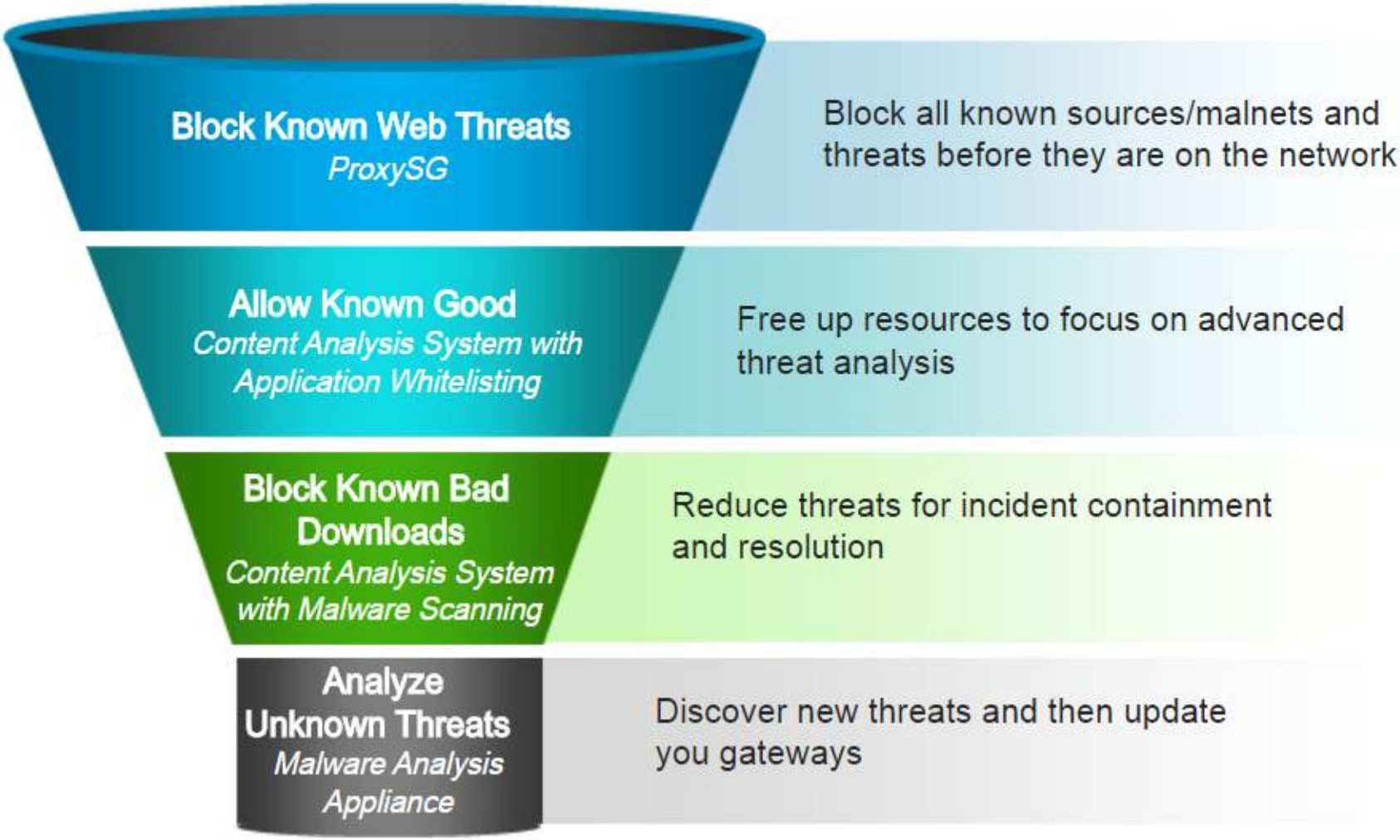
CURRENT SOLUTIONS OPERATE IN SILOS



Technology and Organizational silos limit current defenses

BLUE COAT

INTELLIGENT DEFENSE IN DEPTH



Technology Shifts and Disruptions

Digital Technologies | Cloud Computing | Automation & Robotics | Artificial Intelligence & Cognitive Systems | Internet of Things | Virtual Reality

Scope and Overview

Tech Shifts

- *Technology shifts and trends that are going to disrupt current business models and industries in next 4-5 years; and the impact therefore on Business and Indian IT Industry and how do we take advantage of it.*

Impact

Enabling Technologies

- Analytics/Big Data
- Mobility/Mobile Internet
- Cloud
- Artificial Intelligence
- Connected world (IoT)
- Automation & Robotics
- Augmented & Virtual Reality
- Others?

Industry & Business Themes of Digital Economy

- Finance Services
- Communication
- Media & Entertainment
- High Technology
- Healthcare
- Public service
- Natural Resources
- Retail & CPG
- Travel & Hospitality
- Infrastructure
- Manufacturing & Ind Equipment
- Energy & Utility
- Automotive
- Education

- Seamless Payment
- Connected Healthcare
- Sustainable Manufacturing
- Immersive Learning
- Painless Travelling
- Personalized Consumptions
- Everything as a Service

Cybersecurity Market Sectors

- Anti-Virus/Firewall
- ID Authentication
- Encryption/Privacy
- Risk & Compliance
- Mobile Device Security
- Anti-Fraud Monitoring
- Website Protection
- S/W Code Verification
- AI & Machine Learning
- Enterprise IoT Security
- Cloud Security Services
- Big Data Protection
- RT Log/Event Analytics
- Real-Time Threat Maps
- Smart Biometrics
- Training & Certification

Global Trend is towards ***Adaptive & Intelligent Cybersecurity Solutions/Services***...
....Traditional ***Anti-Virus/Firewall Tools*** no longer fully effective against ***"Bad Guys"***!

Trends, Challenges and Threats in 2018 (1/5)

1. AI and machine learning can boost cyber defenses

- As artificial intelligence and machine learning gathers pace, and starts to impact more and more industries, it's sure to play a bigger role in cybersecurity.

- Because the battle with cyber criminals moves so quickly, machine learning models that can predict and accurately identify attacks swiftly could be a real boon for InfoSec professionals.

- These models need to be trained and honed. However, there is also a risk that AI and machine learning may be exploited by attackers.

Trends, Challenges and Threats in 2018 (2/5)

2. Be proactive about ransomware

- Ransomware has been a growing threat for the last few years, but it continues to claim high profile victims.

- It's not yet clear what everyone learned from the WannaCry Ransomware attacks, highlighted the need to back up regularly, keep patching and updating systems, and strengthen your real-time defenses. If organizations took these simple steps, we could dramatically reduce the impact of ransomware.

3. Handling data breaches gracefully

- It may prove impossible to eradicate data breaches completely, but every organization has the power to lessen the blow by handling the aftermath correctly.

- Equifax gave us a masterclass in how not to handle a data breach earlier this year. By delaying disclosure, misdirecting potential victims, and failing to patch a known vulnerability, one can make a instructive for others in the year ahead.

Trends, Challenges and Threats in 2018 (3/5)

4. The IoT is a weak link

- We're rolling out more and more sensor-packed, internet-connected devices, but the Internet of Things remains a major weak point for defenses.

- All too often these devices lack basic security features, or they aren't properly configured and rely upon default passwords that can give attackers easy access.

- This in turn is giving rise to botnets, which can be used for volumetric attacks, to exfiltrate stolen data, to identify further vulnerabilities, or for brute force attacks. We need to properly secure the IoT or it will continue to be a big issue in 2018.

Trends, Challenges and Threats in 2018 (4/5)

5. There's still a skills shortage

- The dearth of skilled cybersecurity professionals continues to be a major problem for many organizations.
- Even with average InfoSec salaries soaring, there are thousands of vacant positions.
- This is leading many companies to engage external cybersecurity services and virtual CISOs. We expect to see more outsourcing as employers try to find a way to fill the skills gap.

6. Developing a common language

- While the specter of multiple threats looms, there are also positive developments in the cybersecurity realm, not least the creation and adoption of things like NIST's Cybersecurity Framework.
- As more organizations and cybersecurity experts come together to develop a common language, our collective defenses grow stronger.

Trends, Challenges and Threats in 2018 (5/5)

7. Patching and application testing

- It's not shiny or new or exciting, but it should still be top of mind. The number of data breaches in 2017 that were made possible by known vulnerabilities and a sluggish approach to patching is horrifying. It's not enough to identify problems – you must act.

- Application testing falls into the same bucket, in that it's too often ignored.

- If you don't test your security, then you don't know how secure your application is.

- If everyone put a fresh effort into patching and app testing in the coming year, we would see a dramatic drop in data breaches.

Cyber Security HR Requirements

- **Challenge**
  - Acute Shortage of Resource persons
  - Inadequate research in academia
- **Trustworthy System Design: Multidisciplinary Field**
  1. Computer Science
  2. Electronics and Computational System Engineering
  3. Software Engineering
  4. Information Technology
- **Such courses currently not offered in India**
  - Courses can be developed
  - Offered over NKN in MOOC model

Human Resource Development

- Specialists in Trustworthy Information Systems Engineering

- Build Curriculum at UG/PG/PhD Levels
- Courses should be offered in three tracks
  - Systems Area
    - Focus on Attacks from within the system boundary with an emphasis on platform, operating systems, and secure system development.
  - Networks Area
    - Focus on protecting information assets from network-based intrusion and from attacks that are primarily focused on remote exploitation of protected systems.
    - Cybersecurity approaches that are effective in this paradigm should be explored in depth and various defensive approaches should be investigated.
  - Analysis Area
    - Focus on both the systems and networks tracks. Analysis courses study low-level behavior, code, and data to understand anomalies and develop the ability to identify unexpected patterns and malicious events.

The Future of Cyber security Education is Bright

- Emerging challenges will drive the needs in cybersecurity – *Understand the market needs*

- Employers will expect workers to know and apply industry best practices and perspectives - *Align academics to the future expectations*

- The roles are expanding for incoming cybersecurity workforce - *Prepare students for the new roles*

- Resources are emerging to assist academic staff and graduates to understand the needed skill and opportunities – *Empowered students to be self-sufficient in tracking employment demands*

I·C·S
The Institute for Cyber Security

Cyber Security Research

- Foundations
  - Security Models
  - Formal methods
  - Cryptography
- Application-Centric
  - Secure information sharing
  - Social computing
  - Health care
  - Data provenance
- Technology-Centric
  - Cloud computing
  - Smart grid
  - Trusted computing
- Attack-Centric
  - Botnet and malware analysis
  - Complex systems modeling
  - Zero-day defense
  - Moving target defense

CYBER SECURITY HIERARCHY IN INDIA (1/2)

PM OFFICE/CABINET SECY (PMO/CAB SEC)	MINISTERY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANIZATION (NGO)
National Security C0uncil (NSC)	National Cyber Corrd Centre (NCCC)	Ambassadors & Ministers	Tri Service Cyber Commad	Department Of Information Technology (DIT)	Cyber Security And Anti Hacking Organisation (CSAHO)
National Technical Research Org (NTRO)	Directorate of Forensic Science (DFS)	Defence Attaches	Army (MI)	Department of Telecom (DoT)	Cyber Society of India (CySI)
National Critical Info Infrastructure Protection Centre (NCIIPC)	National Disaster Mgt Authority (NDMA)	Joint Secretary (IT)	Navy (NI)	Indian Computer Emergency Response Team CERT-IN	Centre of Excellence for Cyber Security Research & Development in India (CECSRDI)
Joint Intelligence	Central Forensic Science Lab (CFSLs)		Air Force (AFI)	Educational Research Network (ERNET)	Cyber Security of India (CSI)

CYBER SECURITY HIERARCHY IN INDIA (2/2)

PM OFFICE/CABINET SECY (PMO/CAB SEC)	MINISTERY OF HOME AFFAIRS (MHA)	MINISTRY OF EXTERNAL AFFAIRS (MEA)	MINISTRY OF DEFENCE (MOD)	MINISTRY OF COMMON INFO TECHNOLOGY (MCIT)	NON GOVT ORGANIZATION (NGO)
National Crisis Management Committee (NCMC)	Intelligence Bureau (IB)		Def Info Assurance & Research Agency (DIARA)	Informatics Center (NIC)	National Cyber Security of India (NCS)
Research & Analysis Wing (RAW)			Defence Intelligence Agency (DIA)	Centre for Development of Advanced Computing C-DAC	Cyber Attacks Crisis Management Plan of India (CACMP)
Multi Agency Center			Defence Research Dev Authority (DRDO)	Standardisation, Testing and Quality Certification (STQC)	
National Information Board (NIB)					

Recommendations on Cybersecurity Framework for States (1/4)

P-P-P Model for Cybersecurity

- State Cybersecurity Framework shall be envisaged in P-P-P Model
- Government shall partner with the private sector and the scademia to strengthen cybersecurity posture of the state

Information Security Policy and Practices

- IS Policies & practices shall be mandated at govt. functionaries & its service providers
- Security Audit Adhering to international standards applicable for all govt. websites, applications before hosting and publishing
- Govt. to ensure ISPs operating in the state shall deploy cybersecurity plans in line with State cybersecurity policy

Recommendations on Cybersecurity Framework for States (2/4)

State Computer Emergency Response Team

- Establishment of the State CERT to operate in conjunction I-CERT and coordinate with NCIIPC
- Cybersecurity drills shall be carried out under the supervision of I-CERT

Identity Theft and Security Incident Prevention

- State cybersecurity framework to support strategy and implementation mechanisms to prevent digital impersonation and identity theft and the security incidents

Recommendations on Cybersecurity Framework for States (3/4)

Assurance Framework

- Framework of assurance shall be established to provide guidance on security certifications, qualification criteira and prescribe security audits of gov. ICT systems, Projects & applications

Security Budget

- Govt. agencies implementing IT Projects shall allocate appropriate budget towards compliance with the security requirement of IT Act 2000 and State cybersecurity policy, ISMS, security solution procurement and trainings.

Recommendations on Cybersecurity Framework for States (4/4)

Information Sharing

- State Information Sharing Network for CII shall be established

Capacity Building and Awareness

- Govt. shall take appropriate steps for enhancing awareness of citizens and small business for cybersecurity
- Cybersecurity Capacity building and training for professional, extending ISEA program, introducing curricula academia and organizing conferences
- Strengthening LEAs through training, establishment of forensics labs, etc.

Towards 2025 : *"Smart Security Solutions"*

- The Application of Artificial Intelligence and Machine Learning allows us to develop ***"Smart Security Solutions"*** as follows:

*……."**Smart Security Solutions**" typically possess the following features:*

1) ***Space-Time Awareness:*** Location (GPS) & Real-Time Clocks
2) ***Learning, Adaptation & Self-Organisation:*** Real-Time Intelligence
3) ***Massive Memory & Storage:*** Local & Remote Cloud Storage
4) ***Sustainability:*** Embedded Security – *Everywhere in the Network!*
5) ***Scalable Networked Architecture:*** Smart Architectures will need to scale in space & time from micro cells to macro solutions
6) ***Decision Focus:*** "Knowledge Lens" for Data Mining & "Big Data" from Global Social Networks, Search & On-Line Trade & Commerce
7) ***Systems Integration:*** Cyber and Physical Solutions & Operations

THANK YOU