Cyber Security Issues ??
Information Security with Rubik's Cube Model

By,

Mr. Kumar Pudashine (MEng, AIT, Bangkok)
PMP, CISA, CISM, CRISC, CDCP, CEH, CNDA, ITIL, COBIT, CCNP (Enterprise), ISO 27001:2022 LA, JNCIA, AcitivIdentity Certified
IEEE, IEEE Computer Society, ISACA, PMI Member
Kathmandu, Nepal

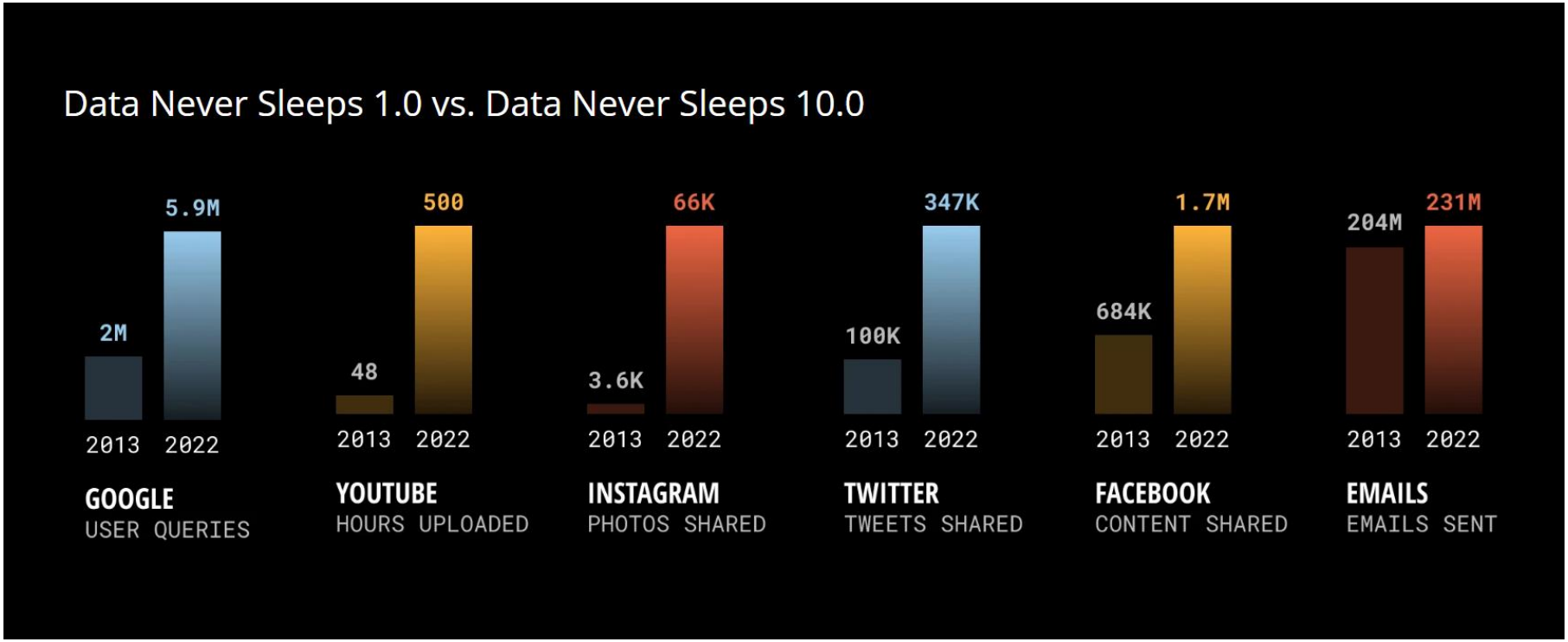
January 2025

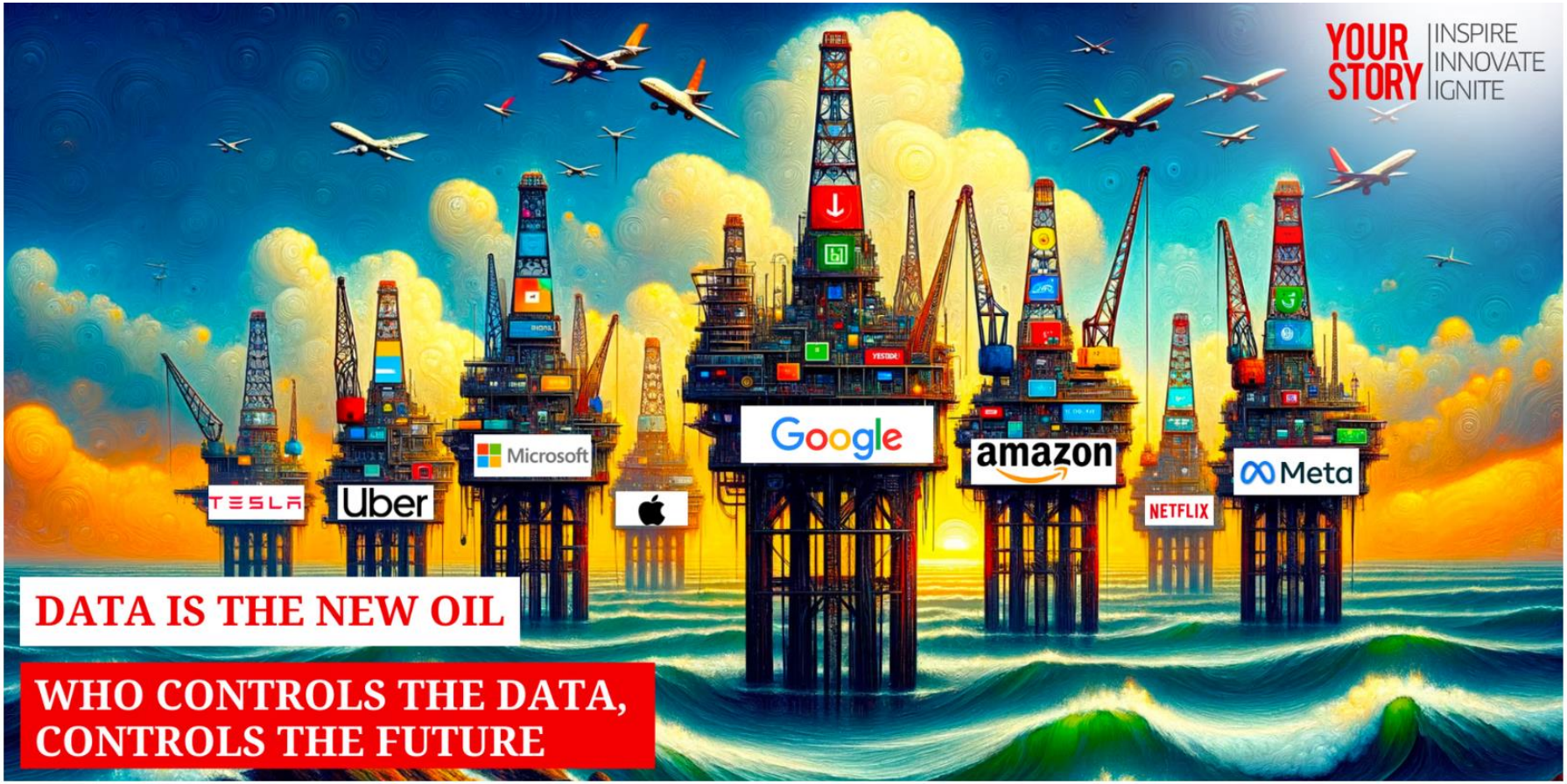
Polling Question

Do you face any Information Security Breach within Six Month Period ?

- ✓ Yes
- ✓ No
- ✓ Don’t Want to Disclose

How much data is generated *every* minute?

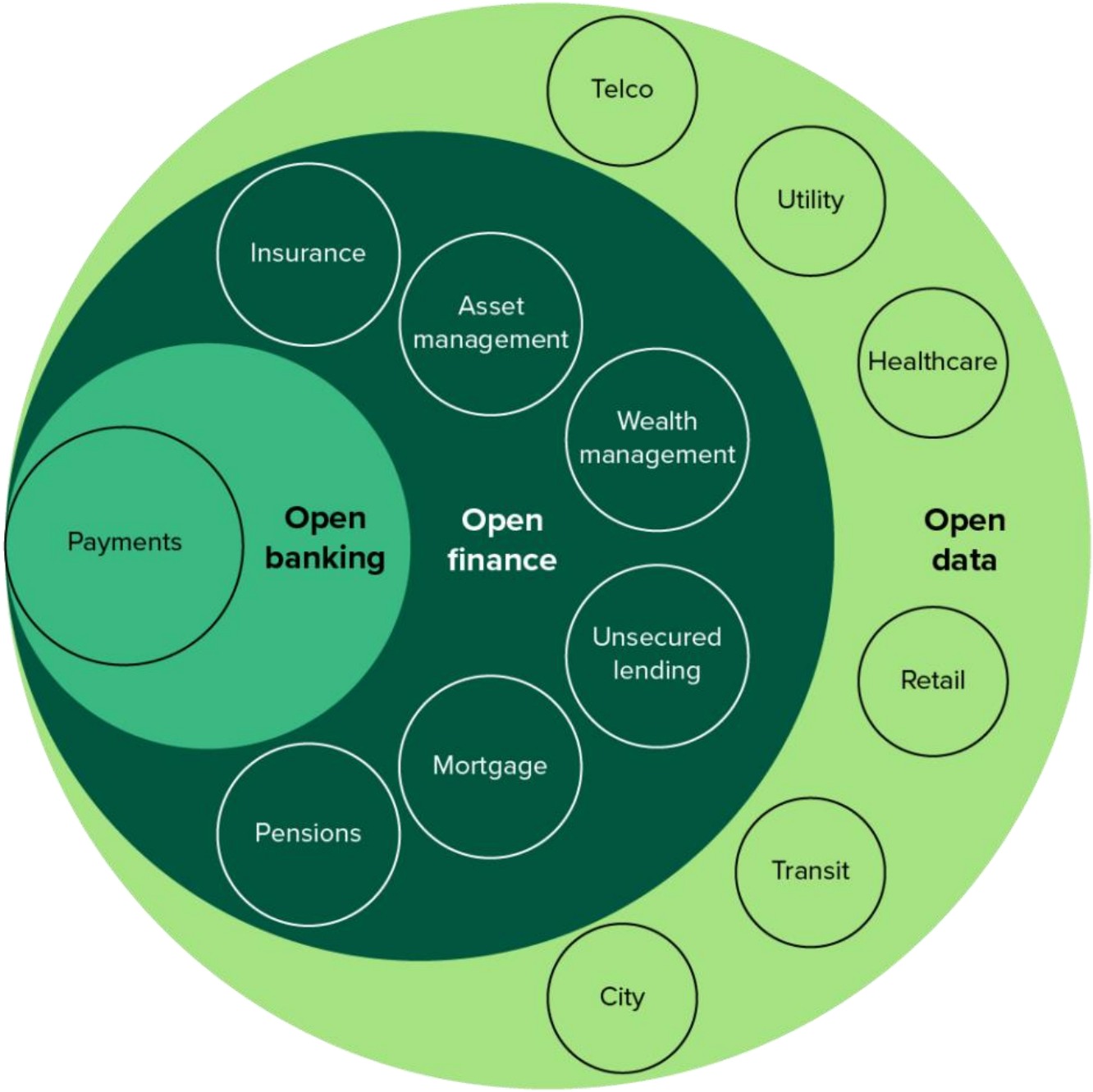


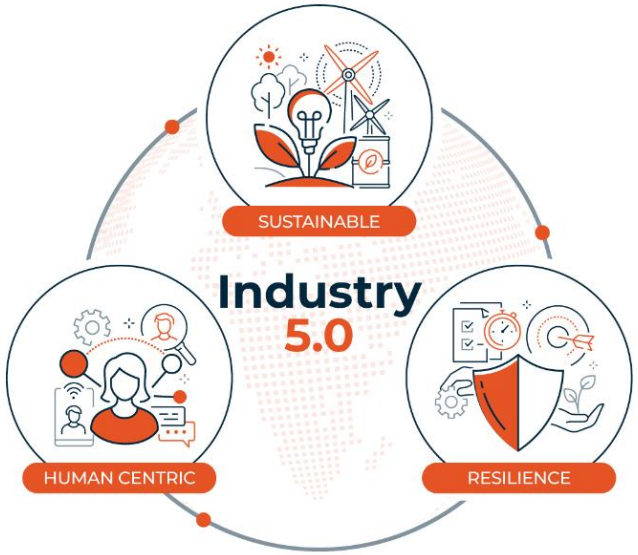


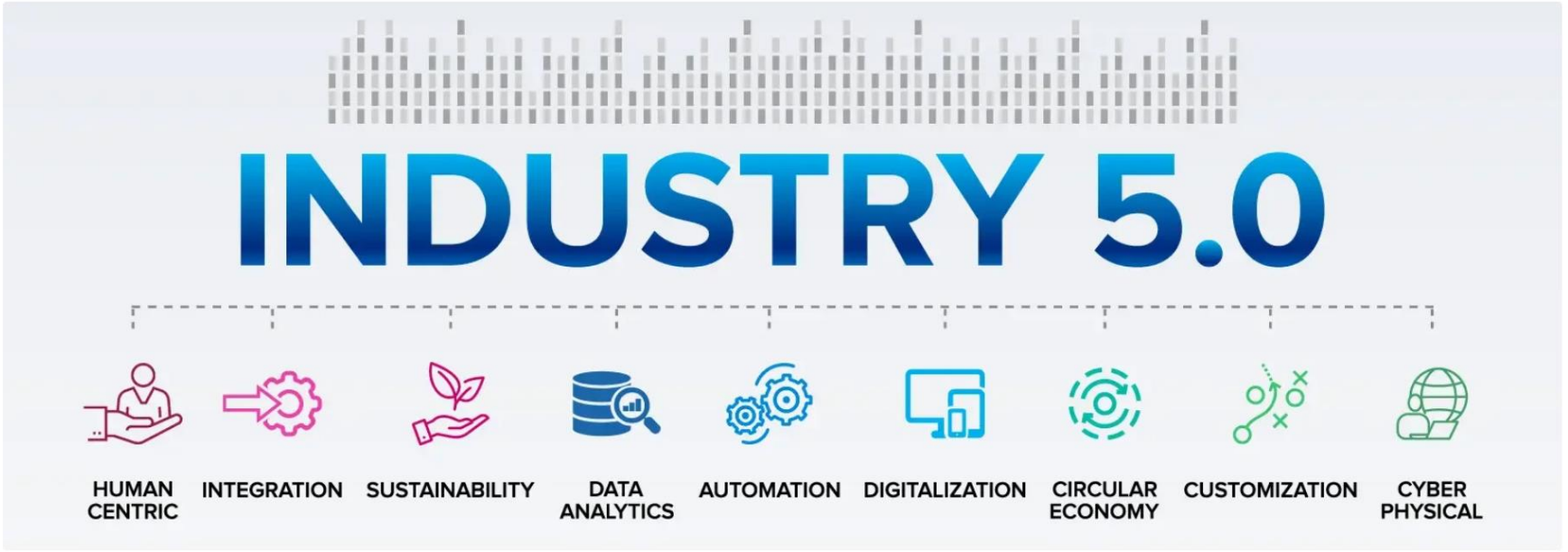
Monday February 19, 2024 , 3 min Read

Reference: https://yourstory.com/2024/02/data-new-oil-controls-data-controls-future


AIRBNB
GUESTS BOOK
747 STAYS
AMAZON
SHOPPERS SPEND
$455K
X
USERS SEND
360K
TWEETS
6.3M
SEARCHES
HAPPEN ON
GOOGLE
WHATSAPP
USERS SEND
41.6M
MESSAGES
LINKEDIN
USERS SUBMIT
6,060
RESUMES
VIEWERS WATCH
43 YEARS
OF STREAMING
CONTENT
3,720
USERS DOWNLOAD
INSTAGRAM
THREADS
CYBER-
CRIMINALS
LAUNCH 30 DDOS ATTACKS
EVERY MINUTE
01:00
OF THE DAY
PRESENTED BY
DOMO
CHATGPT
USERS SEND
6,944 PROMPTS
INSTAGRAM
USERS SEND
694K REELS VIA DM
FACEBOOK
USERS LIKE
4M POSTS
DOORDASH
DINERS PLACE
$122K
IN ORDERS
FANS STREAM A
TAYLOR SWIFT
SONG 69.4K TIMES
VENMO
USERS SEND
$463K
IN PAYMENTS
GLOBAL
INTERNET
USERS SPEND
25.1M
HOURS ONLINE
THE AVERAGE
PERSON
PRODUCES
102 MB
OF DATA
PEOPLE TRADE
$398M
IN TREASURY
BONDS
PEOPLE SEND
241M
EMAILS
TWITCH
USERS WATCH
48K
HOURS OF CONTENT

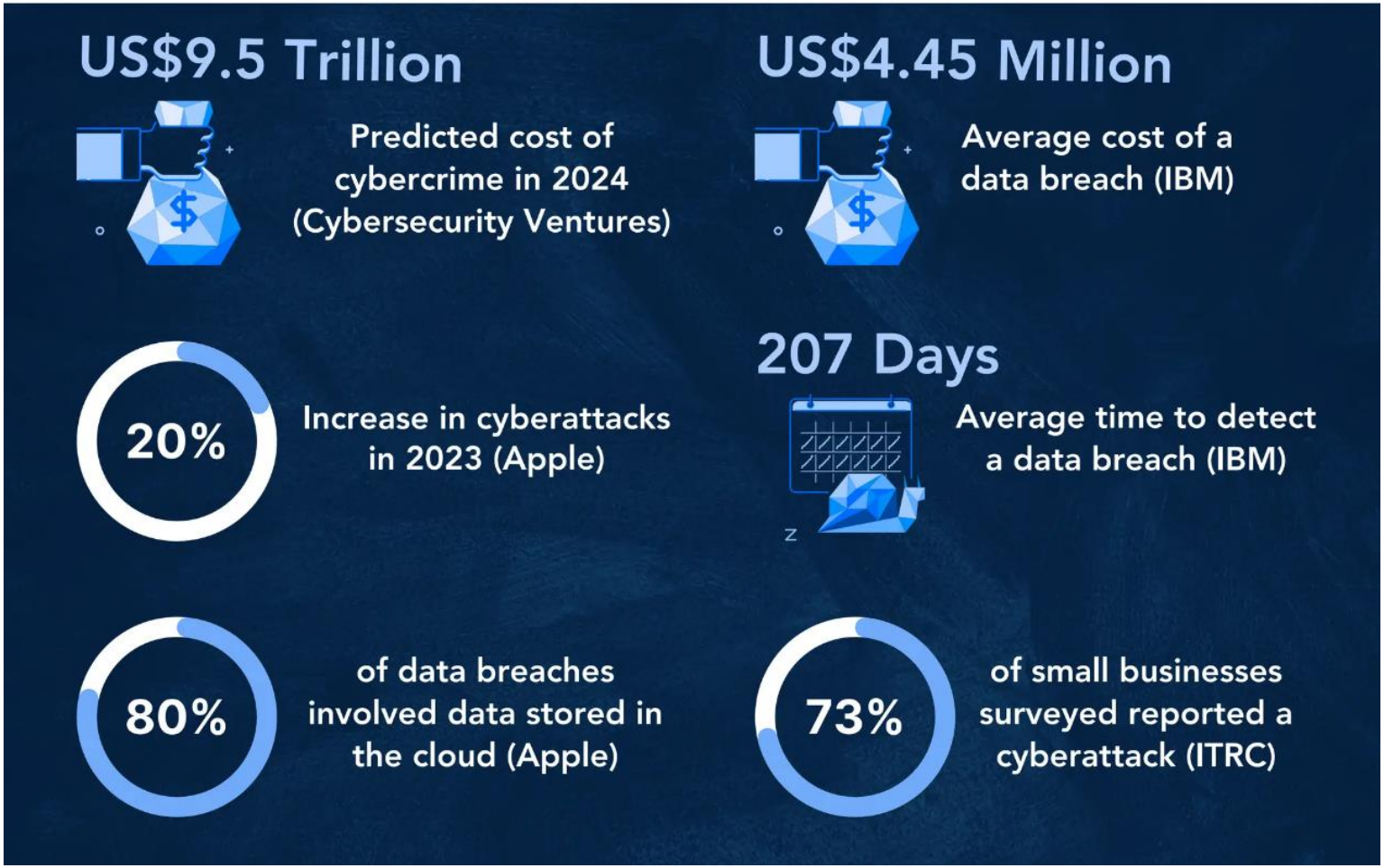

Telco
Utility
Insurance
Asset management
Healthcare
Wealth management
Payments
Open banking
Open finance
Open data
Unsecured lending
Retail
Mortgage
Pensions
Transit
City





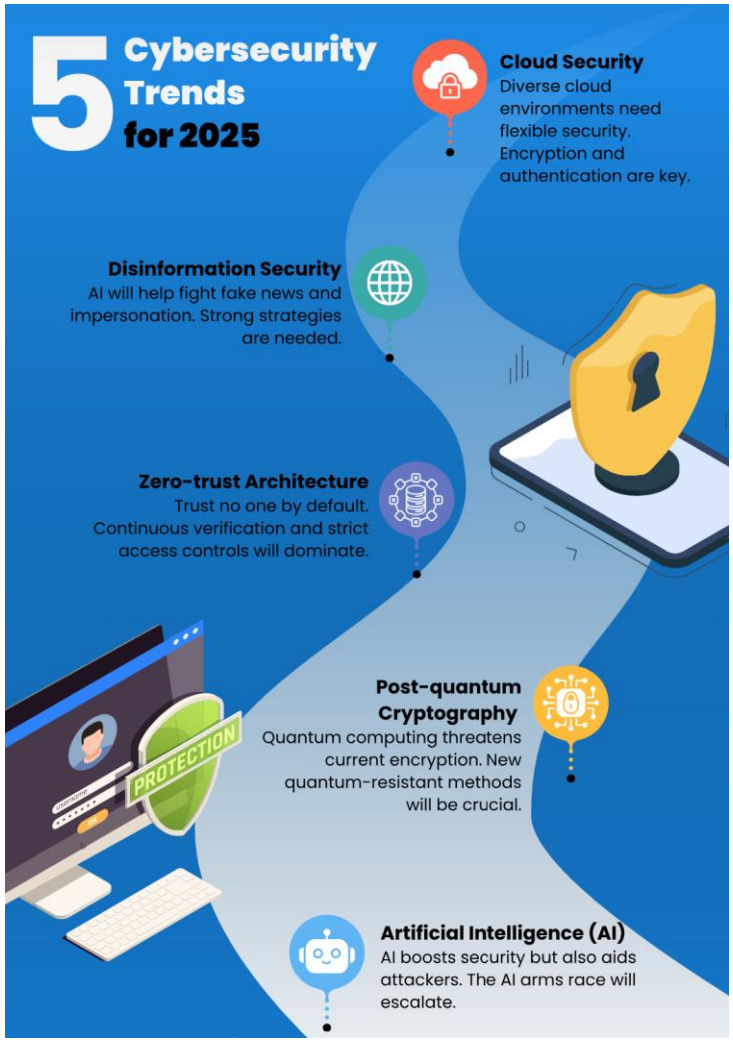
https://hgs.cx/blog/what-is-industry-5-0-explore-the-key-benefits-and-future-potential/

Cyber Security Trends of 2024



https://www.slideshare.net/slideshow/cyber-security-trends-in-2024-apollo-secure/266709390

Cyber Security Trends of 2025



https://www.proserveit.com/blog/top-5-cybersecurity-trends-for-2025

Cyber Crime Statistics

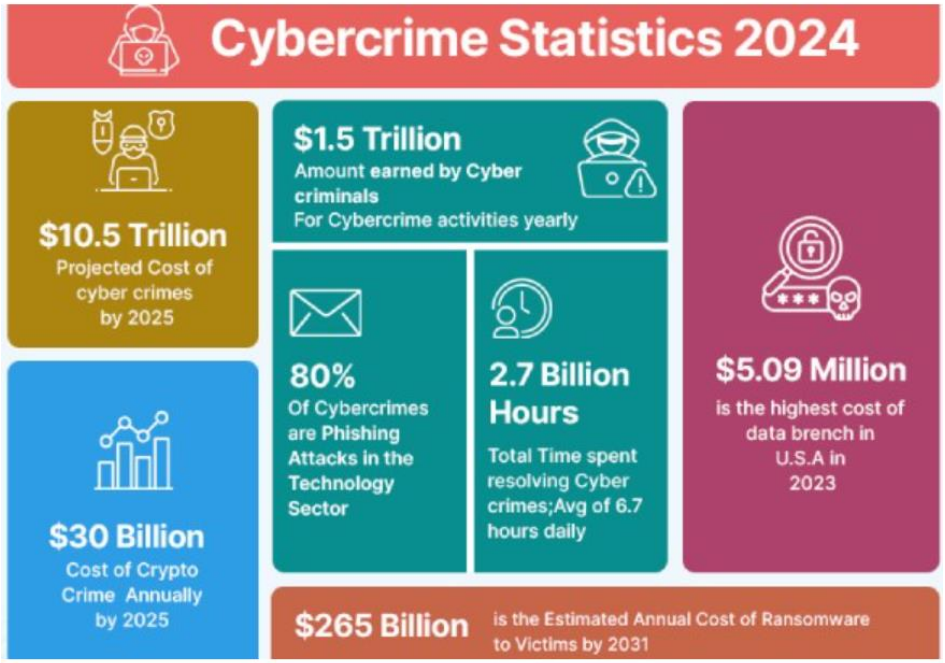
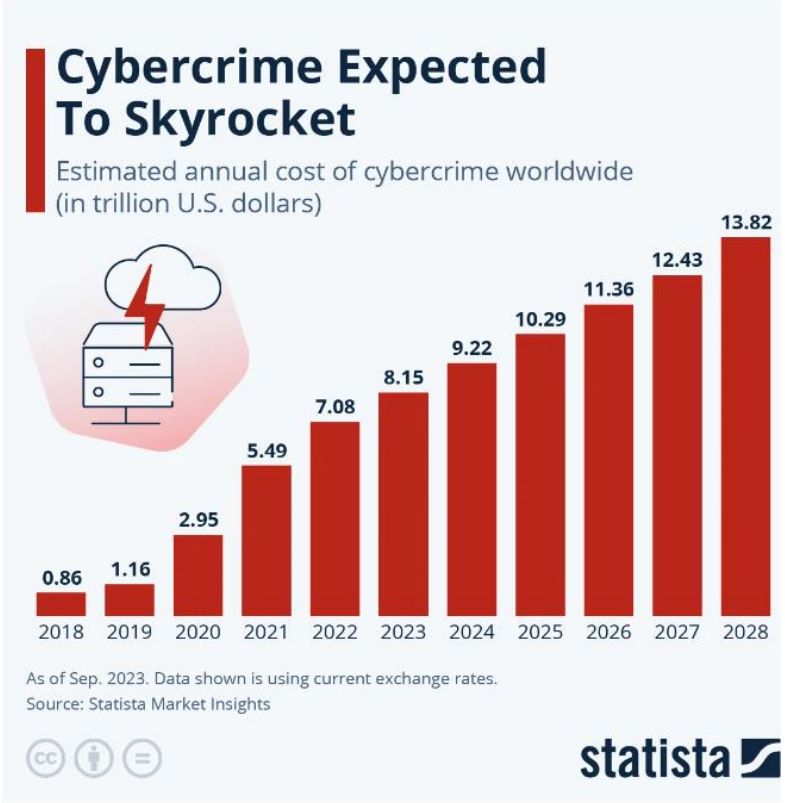


Image sourced from eluminoustechnologies.com



The global projected cost of cybercrime will reach $13.82 trillion in 2028.
via Statista

Cybersecurity News: SecureWorld

Business

Ransomware attack on England's health system highlights life-threatening impact of cybercrime

National Health Service urgently seeks blood donors after transfusions disrupted

Jordan Pearson · CBC News · Posted: Jun 11, 2024 4:00 AM EDT | Last Updated: June 11

A ransomware attack on June 3 that targeted London-based pathology services provider Synnovis severely impacted several hospitals in the city serving two million people, prompting them to declare a critical incident and cancel cancer surgeries and blood transfusions. (Azami Adiputera/Shutterstock)

Does Ransomware Kill Sick People?

TUE | JUN 11, 2024 | 12:28 PM PDT

You probably already know that ransomware is a type of malicious software that encrypts a victim's data, demanding a ransom to restore access. It's a problem that's getting worse all the time, and its impact on healthcare is particularly concerning.

Aside from the inconvenience created for everyone present when hospital systems go offline, the question we need to ask is whether ransomware can actually kill sick people. This might sound grim, but it's an important topic.

Just consider a recent cyberattack on Anna Jaques Hospital in Massachusetts. On Christmas Eve 2023, their electronic health records were knocked offline, forcing them to turn away ambulances. This isn't the first time something like this has happened. In 2020, a patient in Düsseldorf, Germany, died during an ambulance diversion caused by a ransomware attack against the local university hospital.

And, a ransomware-related death in the United States recently went to court.

A baby, Nicko Silar, was born in July 2019 at Springhill Memorial Hospital in Alabama, which was struggling with a ransomware attack at the time.

Cybersecurity News: SecureWorld

Ransomware Attack on Mumbai's Power Grid: Lessons Learned

digiALERT
1,116 followers

+ Follow

November 8, 2023

Open Immersive Reader

The year 2023 witnessed a significant turning point in the realm of cybersecurity as Mumbai's power grid fell victim to a crippling ransomware attack. This event sent shockwaves throughout the cybersecurity community, shining a harsh spotlight on the potential consequences of such attacks on critical infrastructure. In this extensive blog, we will delve deep into the nuances of the ransomware attack on Mumbai's power grid and extract valuable lessons that have far-reaching implications for the world of cybersecurity.

Mumbais Power Grid Ransomware Attack: A Brief Overview

Before we dive into the lessons learned, let's establish a comprehensive understanding of the ransomware attack that unfolded in Mumbai. The attack

CRITICAL INFRASTRUCTURE

European power grid organization hit by cyberattack

The incident affected our office network, says ENTSO-E, as it implements measures to avoid future cyber-incursions

Amer Owaida

12 Mar 2020 • 2 min. read

Reference: https://www.welivesecurity.com/2020/03/12/european-power-grid-organization-entsoe-cyberattack/

https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

Cybersecurity News: Times of India

How hackers are using generative AI to attack Indian businesses

TOI Tech Desk / TIMESOFINDIA.COM / Updated: Mar 26, 2024, 09:47 IST

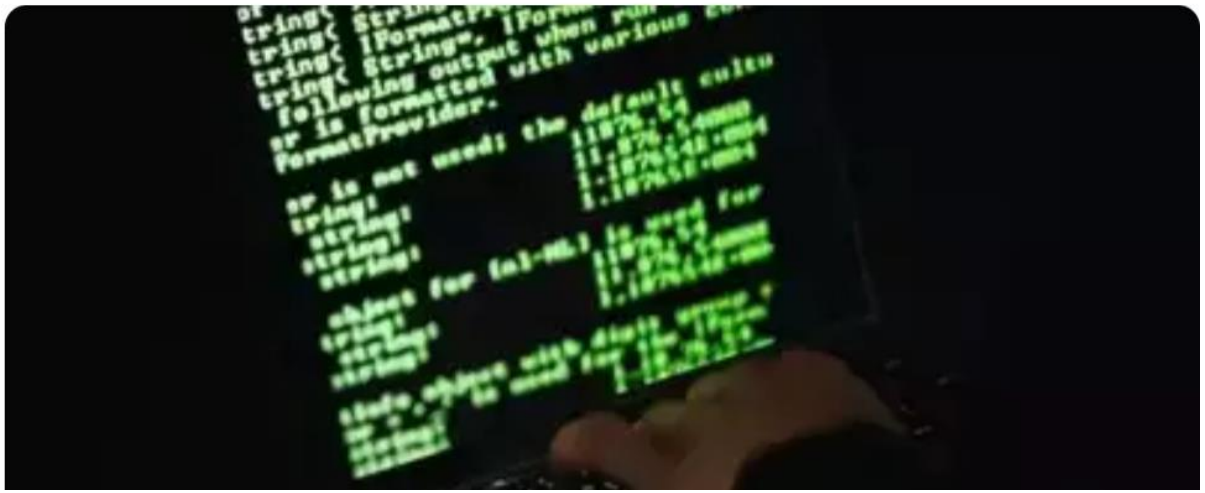
SHARE AA FOLLOW US

Generative AI fuels convincing phishing messages targeting Indian companies through human error. Kaspersky report exposes attacks across email, websites, and social media, luring users to share financial data and spread malware. Scammers exploit fear technique.

Read Less

'It is sickening.. we are tired ... ': Karnataka's CID sleuths swamped with...

India steps up training of foreign military personnel to boost ties



IoT : Internet of Things

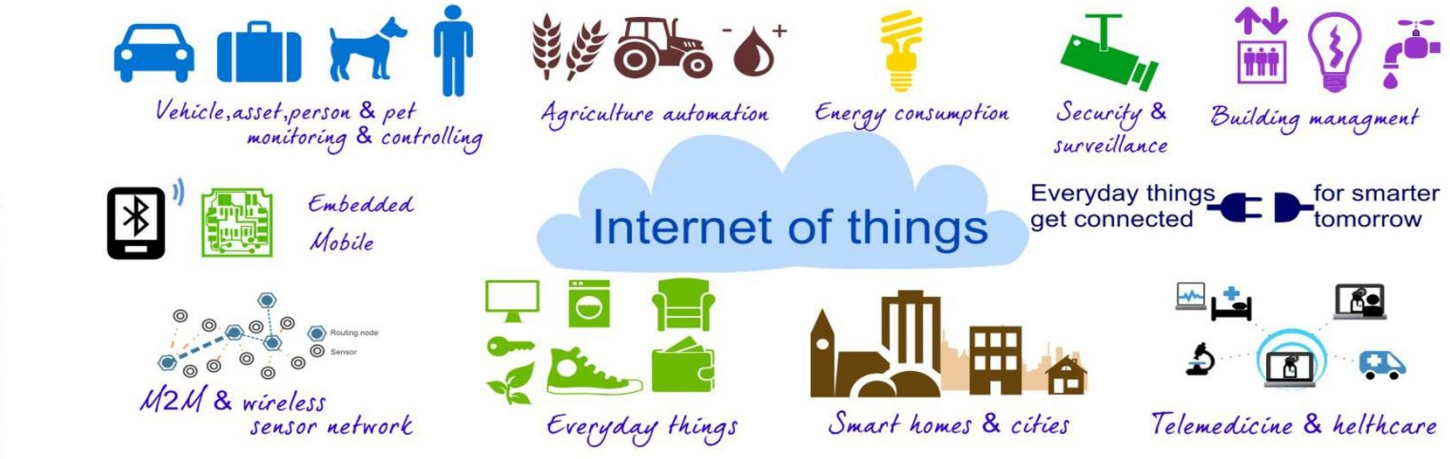
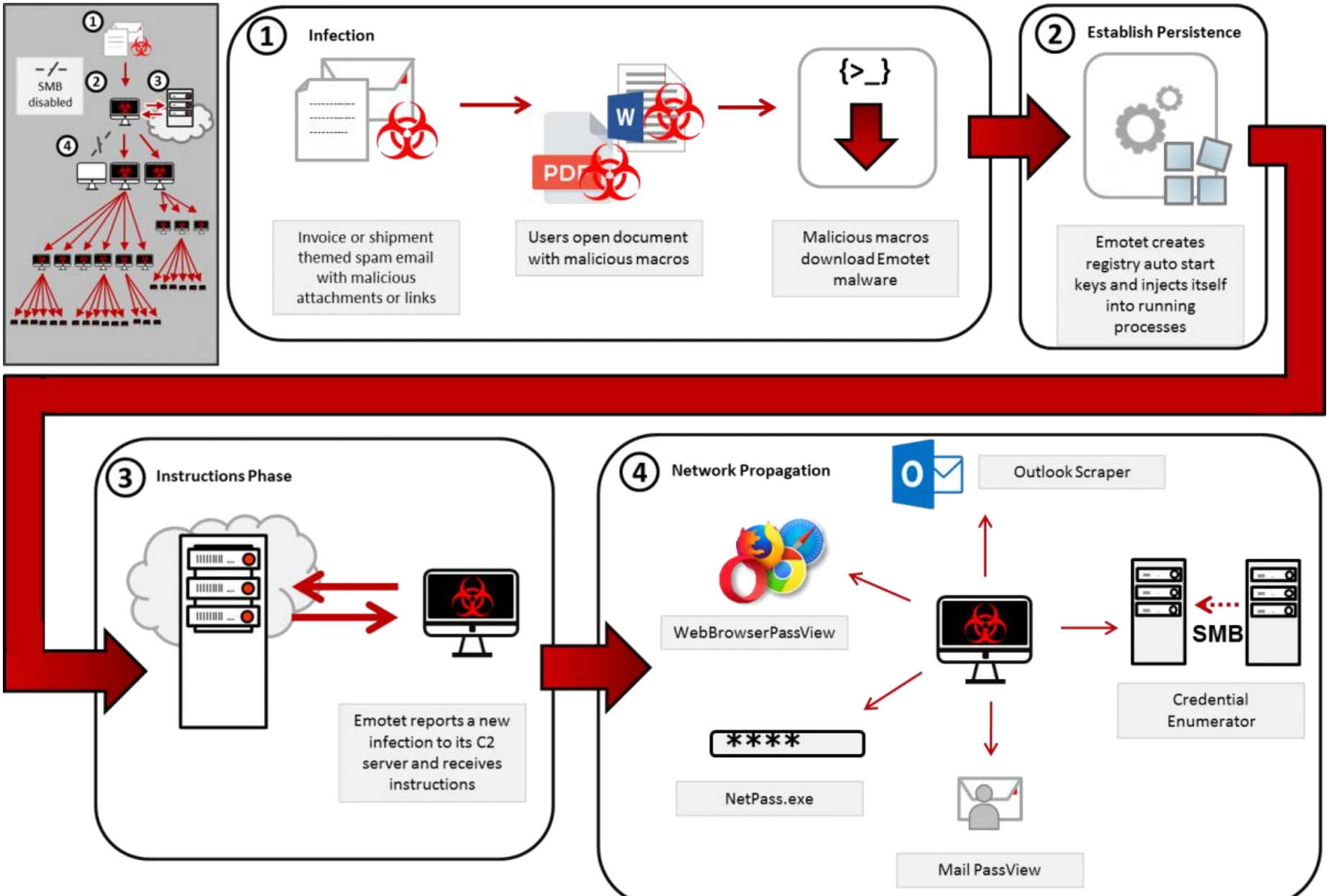


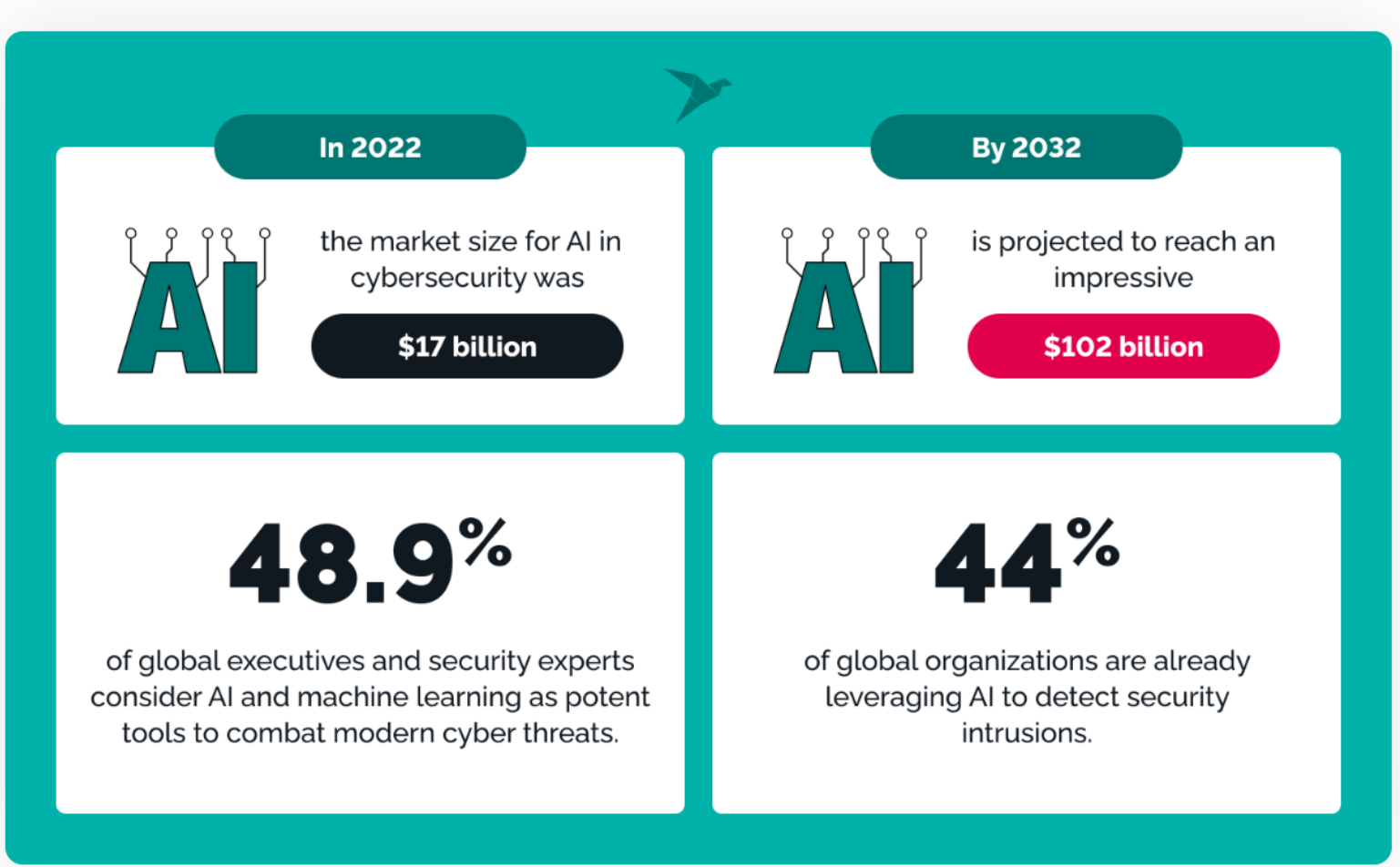
Fig. 1. *Internet of Things and Future Internet. (2014, June 24). Retrieved October 25, 2016, from http://www.slideshare.net/torstenbraun/internet-of-things-and-future-internet iCIS summer workshop Coimbra 2014. Fig. 2. Internet of Things is Already Here [Photograph]. (2011). CISCO IBSG.*


WEB 3.0
POTENTIAL RISKS
https://www.linkedin.com/in/santoshkamane
Lack of governance and oversight
Decentralization could also result in lack of accountability, common policies, best practices, agreements and auditing practices.
Vulnerable smart contracts
Security bugs and exploits are key concerns in smart contracts as it could lead to financial breaches
Unsecure Crypto Wallets
Crypto wallets can be vulnerable to attacks, such as phishing and malware, that can lead to the loss of funds
DAO security
Decentralized Autonomous organizations are key entities on blockchain and can be vulnerable to security flaws in the code.
Interoperability issues
Web3.0 is a new phenomena which is drastically different from web2.0. The interoperability of technologlies and protocols may pose challenges.

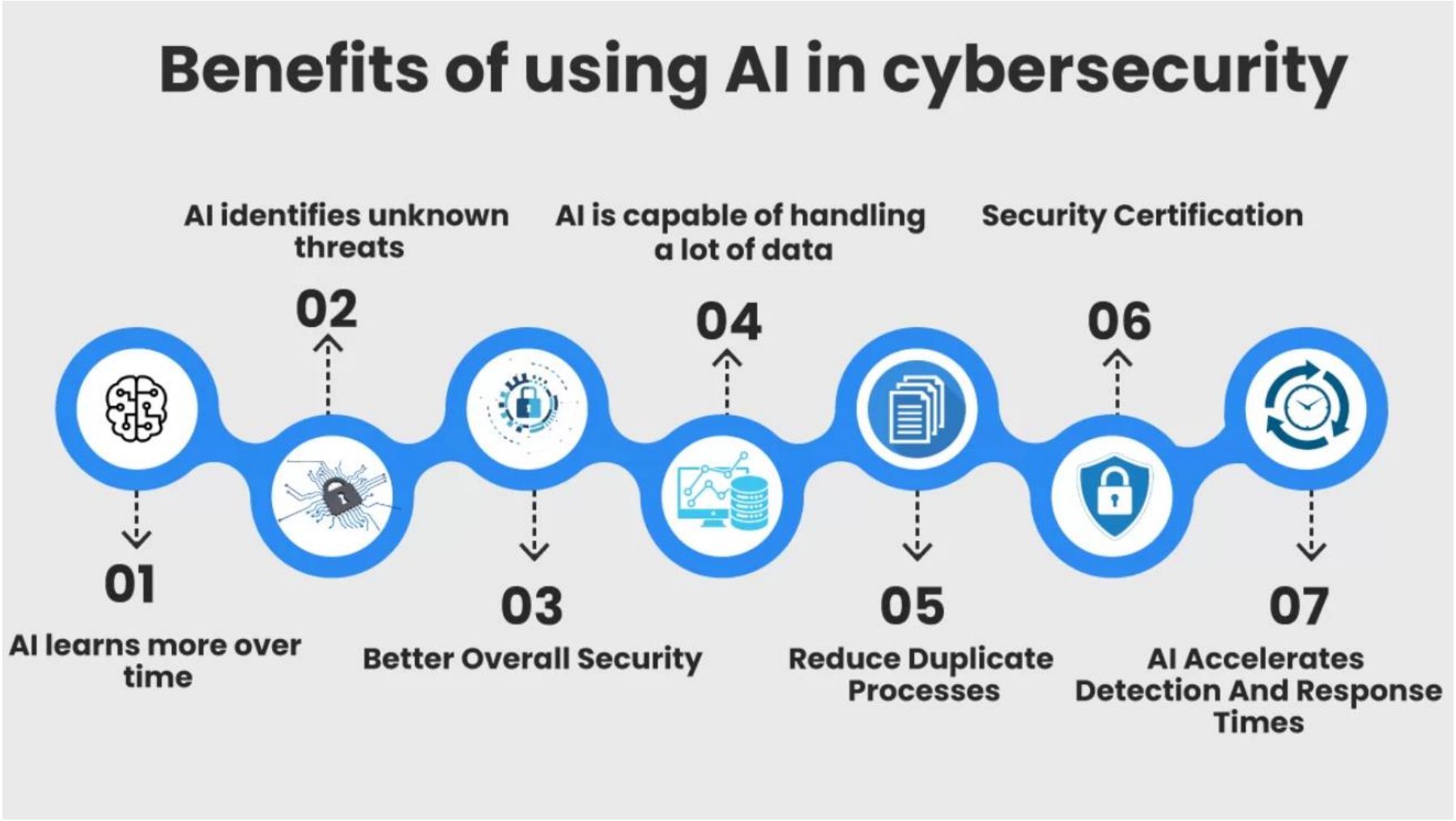
APT : Advanced Persistent Threat



AI Growth



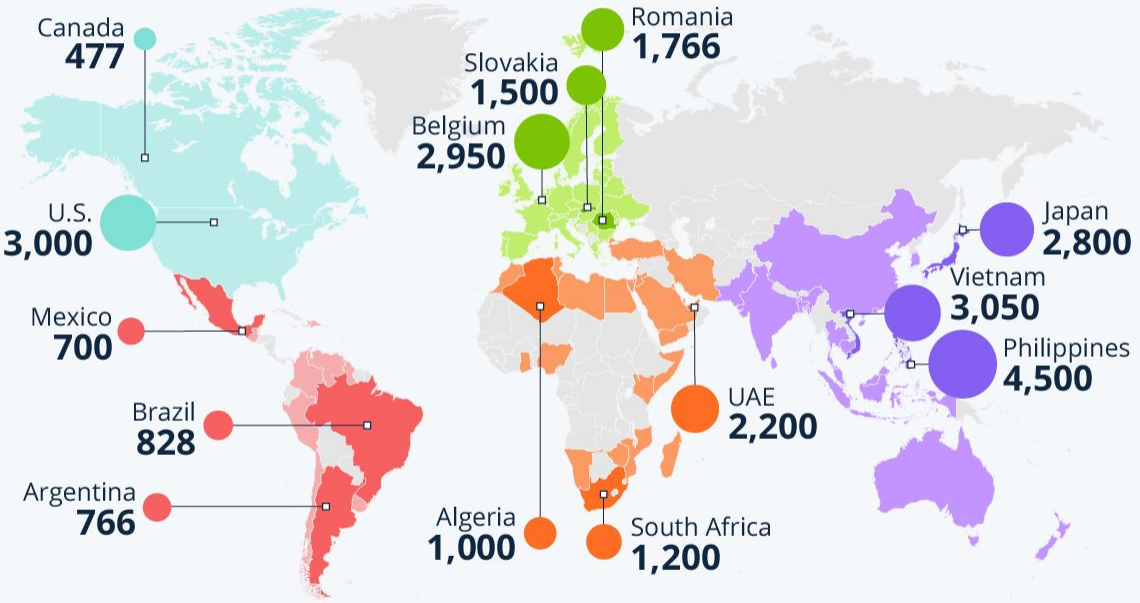
https://www.techmagic.co/blog/ai-in-cybersecurity/



https://hashstudioz.com/blog/benefits-of-using-artificial-intelligence-in-cyber-security/

The Explosive Growth of AI-Powered Fraud

Countries per region with biggest increases in deepfake-specific fraud cases from 2022 to 2023 (in %)*



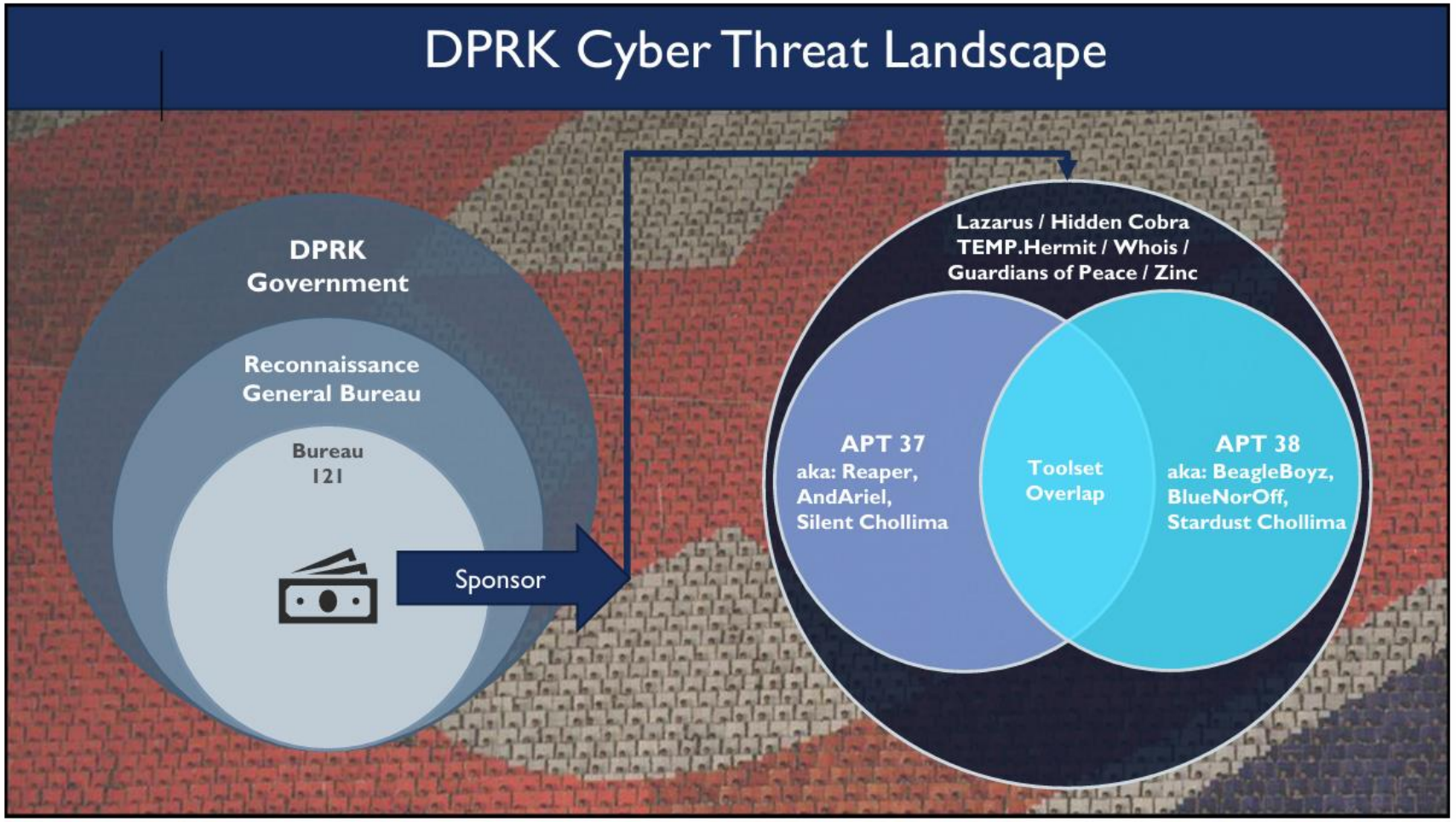
The report analyses +2M cases of identity fraud attempts from 224 countries/territories.
All data is aggregated and anonymized * Regions according to source

Source: Sumsub Identity Fraud Report 2023

statista

https://www.statista.com/chart/31901/countries-per-region-with-biggest-increases-in-deepfake-specific-fraud-cases/

DPRK Cyber Threat Landscape



DPRK Cyber Attacks: Targets

DPRK Cyber Attacks: Targets

CITIZENS

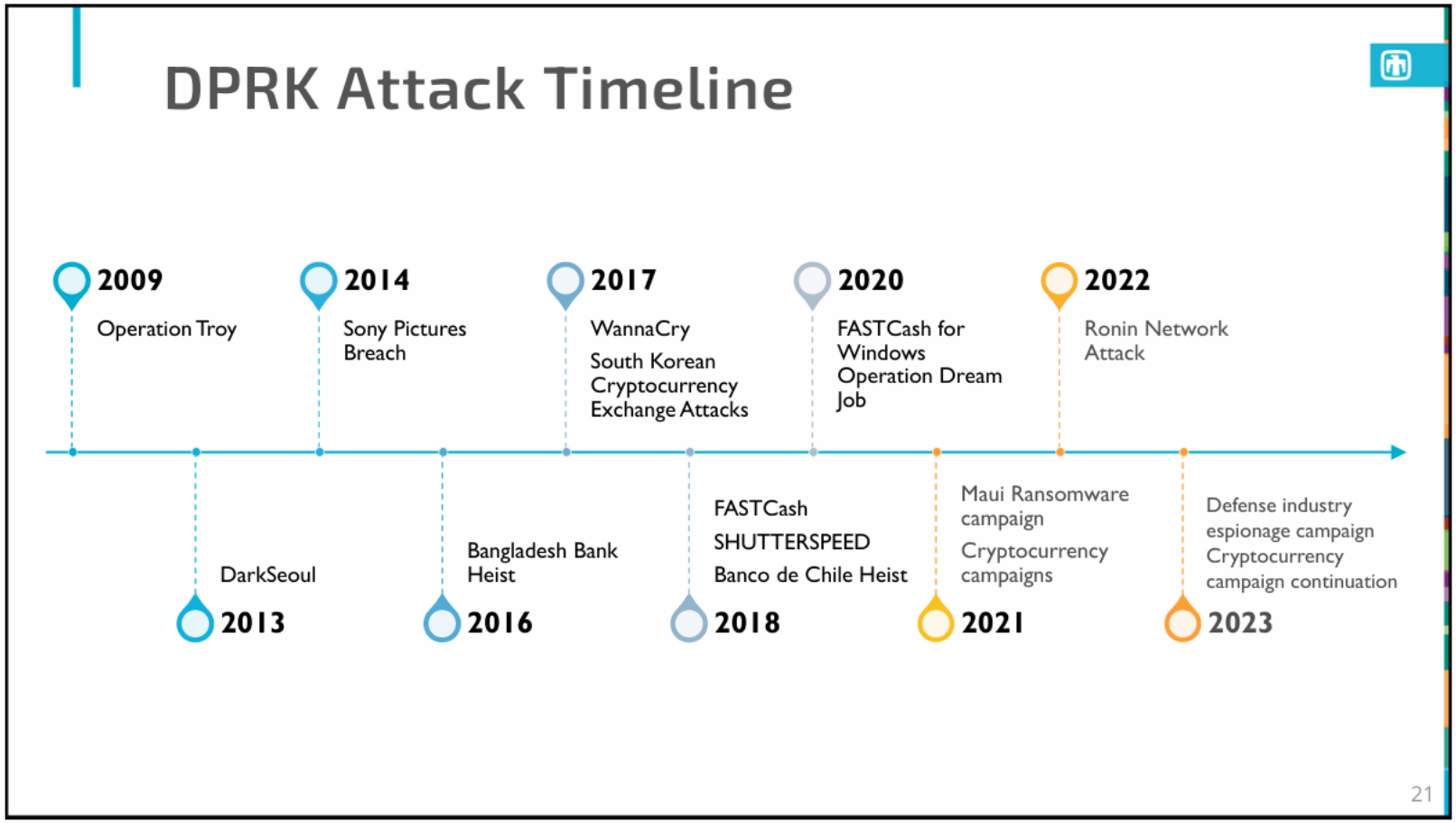
SONY PICTURES

PRIVATE COMPANIES

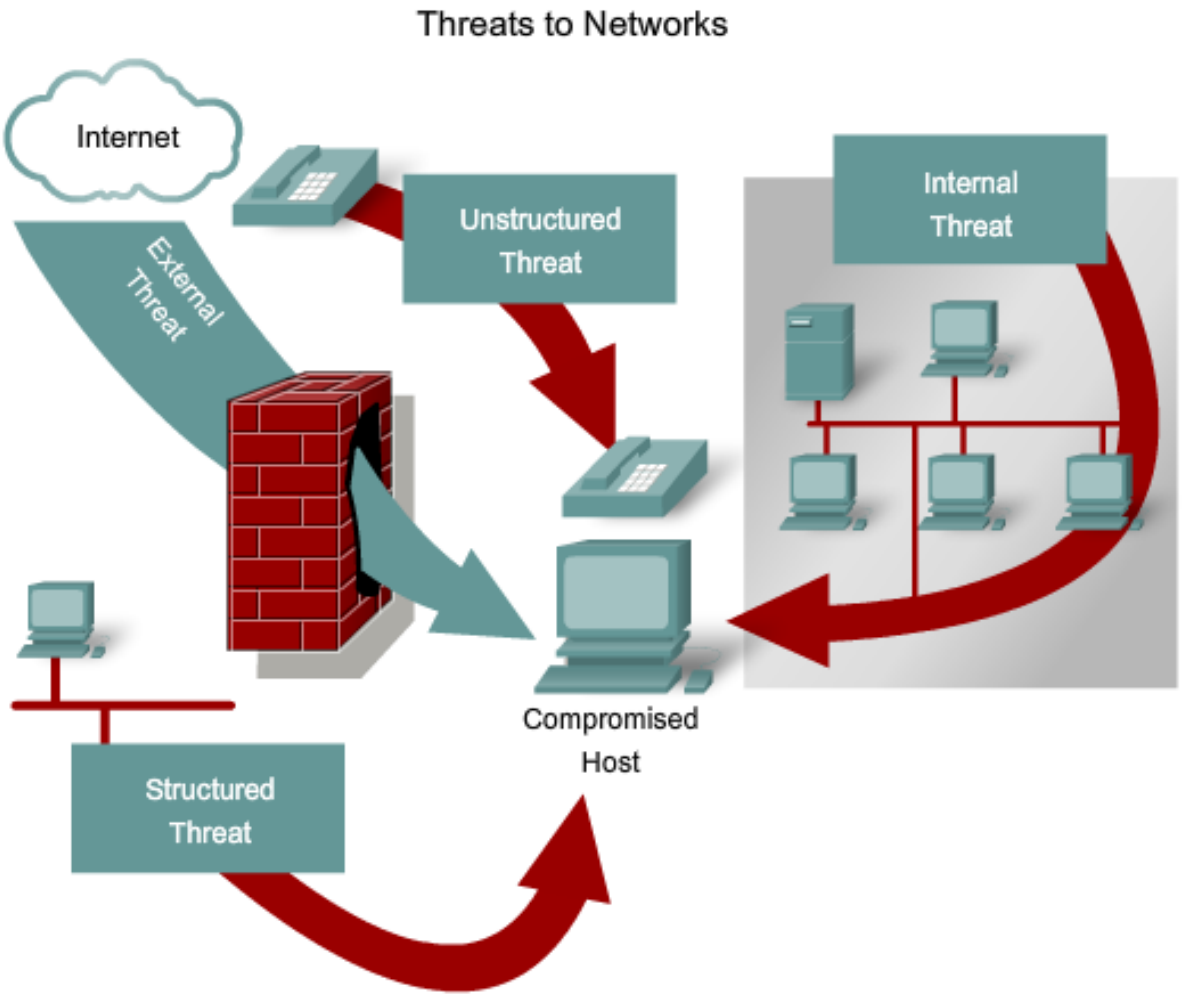
GOVERNMENT AGENCIES

FINANCIAL SECTOR

DPRK Attack Timeline



Sophistication of Threats



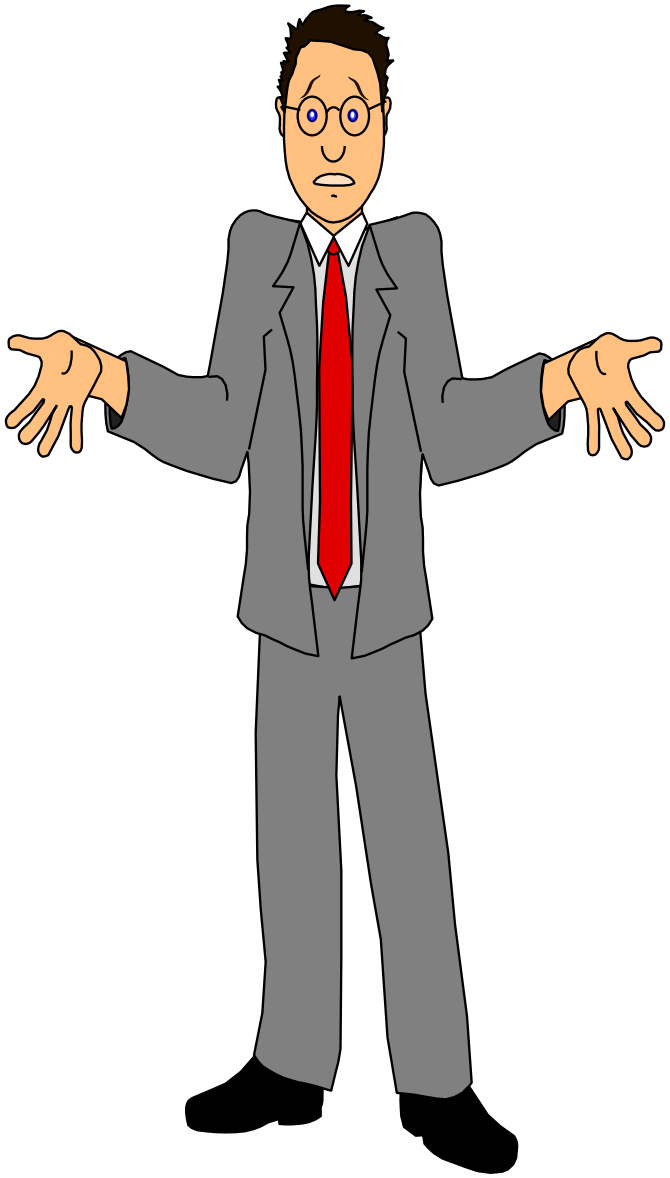
You Will Be Hacked

Be Ready..!!

Risks: 4P(People, Process, Product and Partners)

- Product
  (Technologies: Cloud, ERP, HRIS, CBS)
- People
  (Human Resources : End Users, System Admins etc.)
- Partners
  (Outsourced Vendors)
- Process
  (Policy, Standard Operating Procedures, Guidelines)

Solution Outlines?



Information Security : Defense in Depth Approach

GOVERNANCE & RISK MANAGEMENT

- ISO 27002 Compliant
- Center for Internet Security (CIS) Controls
- 3 Annual Pen Tests
- Privacy Shield Certified
- GDPR / CCPA Compliant
- Enterprise Risk Register
- NIST SP 800-53 Compliant
- SSAE 18 SOC 1 Type 2 Certified
- Standard Information Gathering (SIG)
- Information Security Audit Reports
- Enterprise Incident Response

PLATFORM SECURITY

- Next Generation Firewalls
- Antivirus for Servers
- AES 256 Encryption at Rest
- Segregated Active Directory & VLANS
- Privileged Account Vaulting
- Continuous Vulnerability Scanning & Patch Management
- Secure Data Backups and Disaster Recovery
- Operating Systems Hardening

END USER PROTECTION

- Cybersecurity Awareness Training
- Multifactor Authentication
- Role-Based Access Control
- Simulated Phishing Campaigns

SIEM

- Raw Logs, Endpoint Data & Network Traffic Analytics
- Unified Log Data
- User Behavior Analytics (UBA)
- Suspicious Activity Detection & Alerts

PERIMETER SECURITY

- External Firewalls
- Remote Access
- Spam Filtering
- Threat Intel Feeds
- Remote Authentication Reporting
- Brute Force and DoS Detection
- Data Center Physical Security

ENDPOINT SECURITY

- Automated Microsoft Windows and 3rd Party Application Patch Management
- Antivirus and Endpoint Detection & Response (EDR)
- Remote Monitoring & Management System
- Local Admin Password Solution
- Full Disk Encryption
- Mobile Device Management
- Group Policy Enforcement
- Password Complexity
- Brute Force Prevention

Information : ??

Information is a Virtual Asset which, like other important business assets, has value to an organization and consequently needs to be suitably Protected.

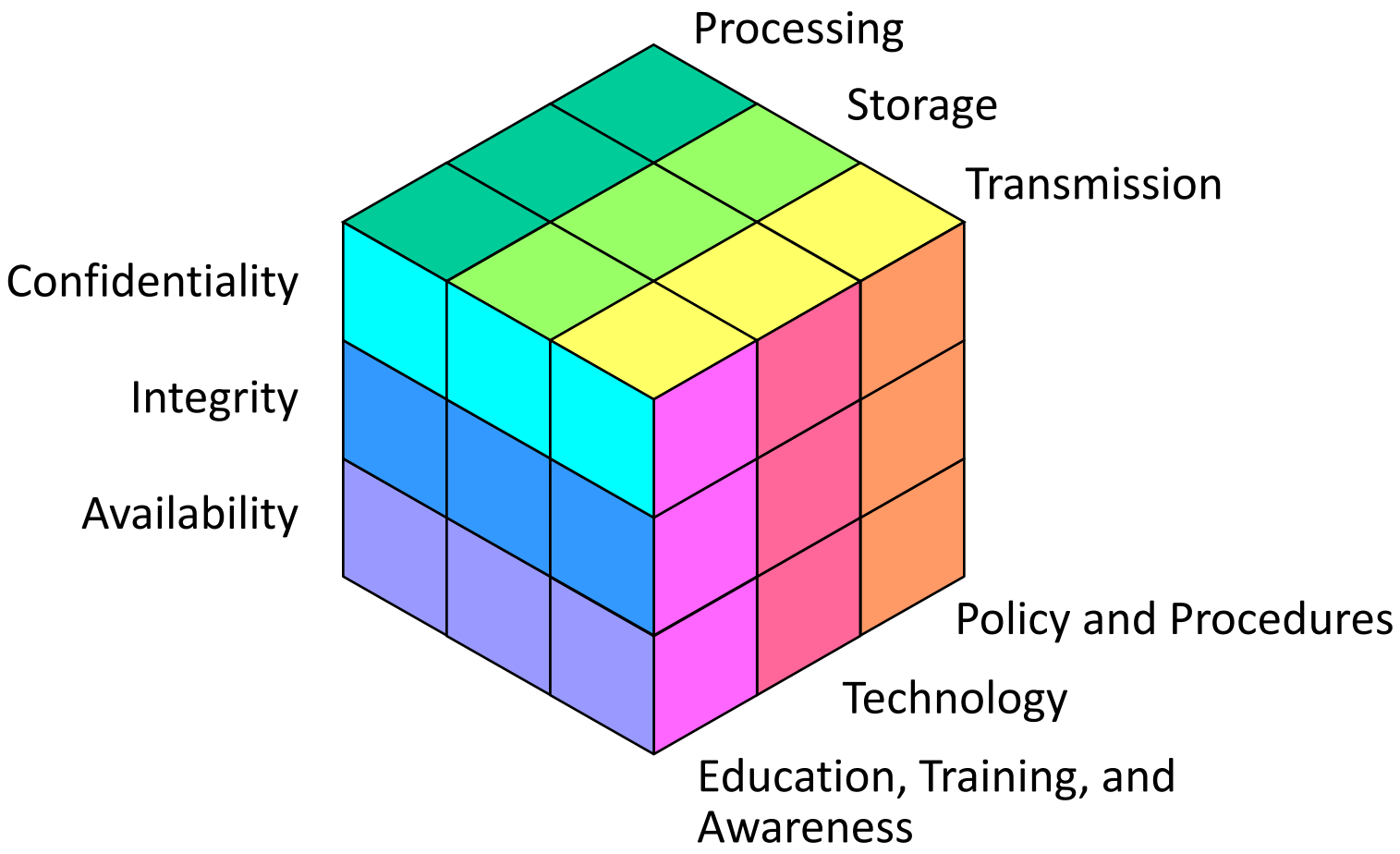
ISO/IEC 27002:2005

Information Security: Key Terms

- Information Security is a process by which Digital Information assets are Protected.

- It is not something you BUY, it is something you DO
  - It's a ***PROCESS*** not a ***PRODUCT***
- It is achieved using a combination of suitable strategies and approaches:
  - Determining the **RISKS** to information and Treating them accordingly (Proactive Risk Management)
  - Protecting **CIA** (**C**onfidentiality, **I**ntegrity and **A**vailability)
  - Avoiding, preventing, detecting and recovering from incidents
  - Securing people, processes *and* technology … not just IT!

Information Security: Rubik's Cube Model

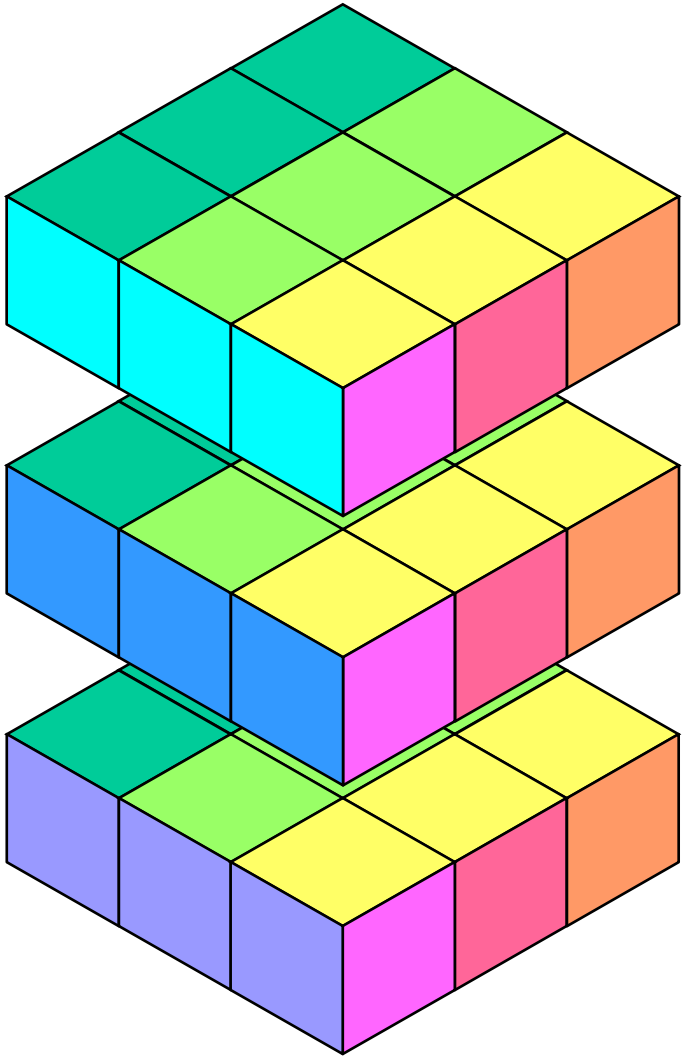


Information Security Properties

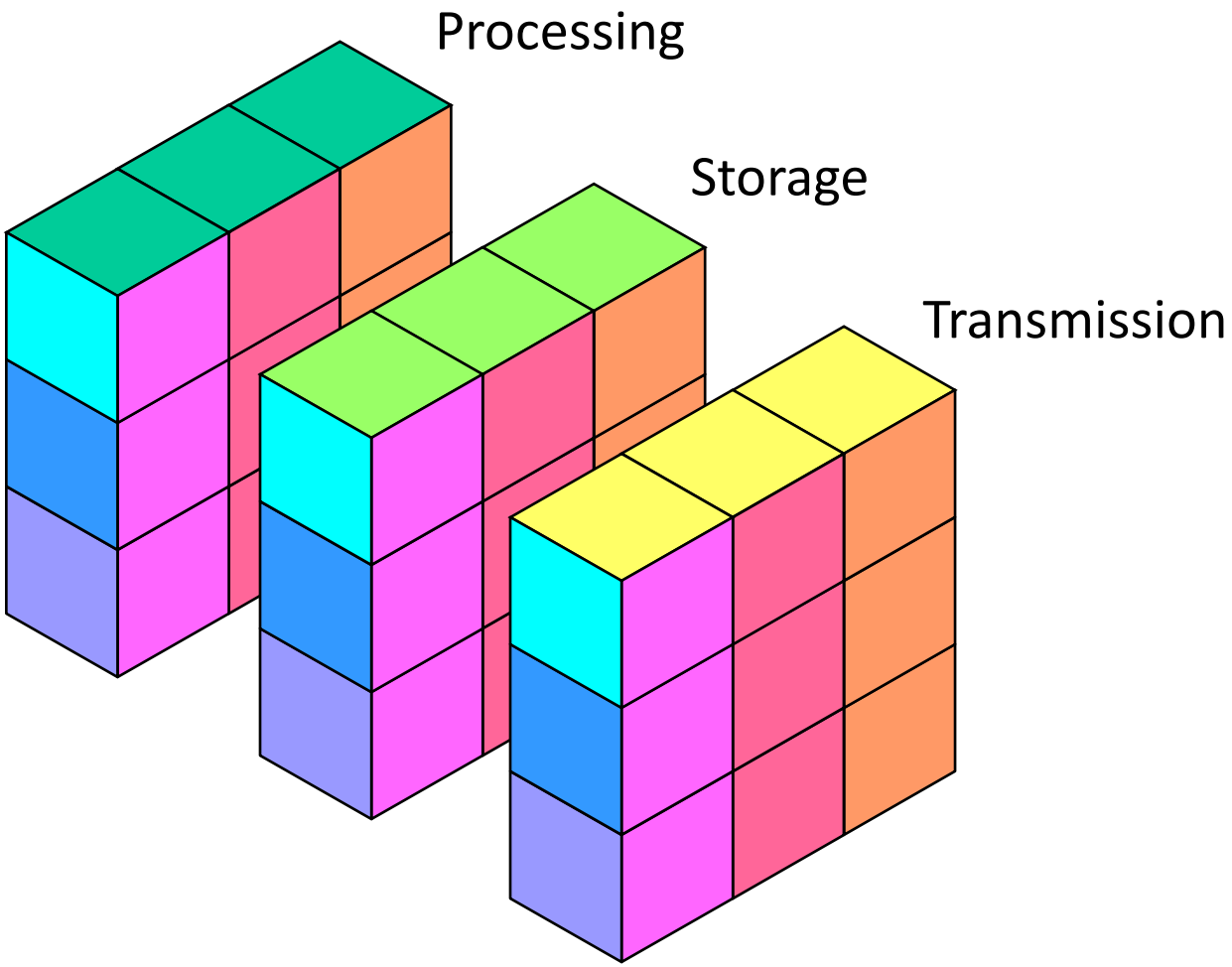
Confidentiality

Integrity

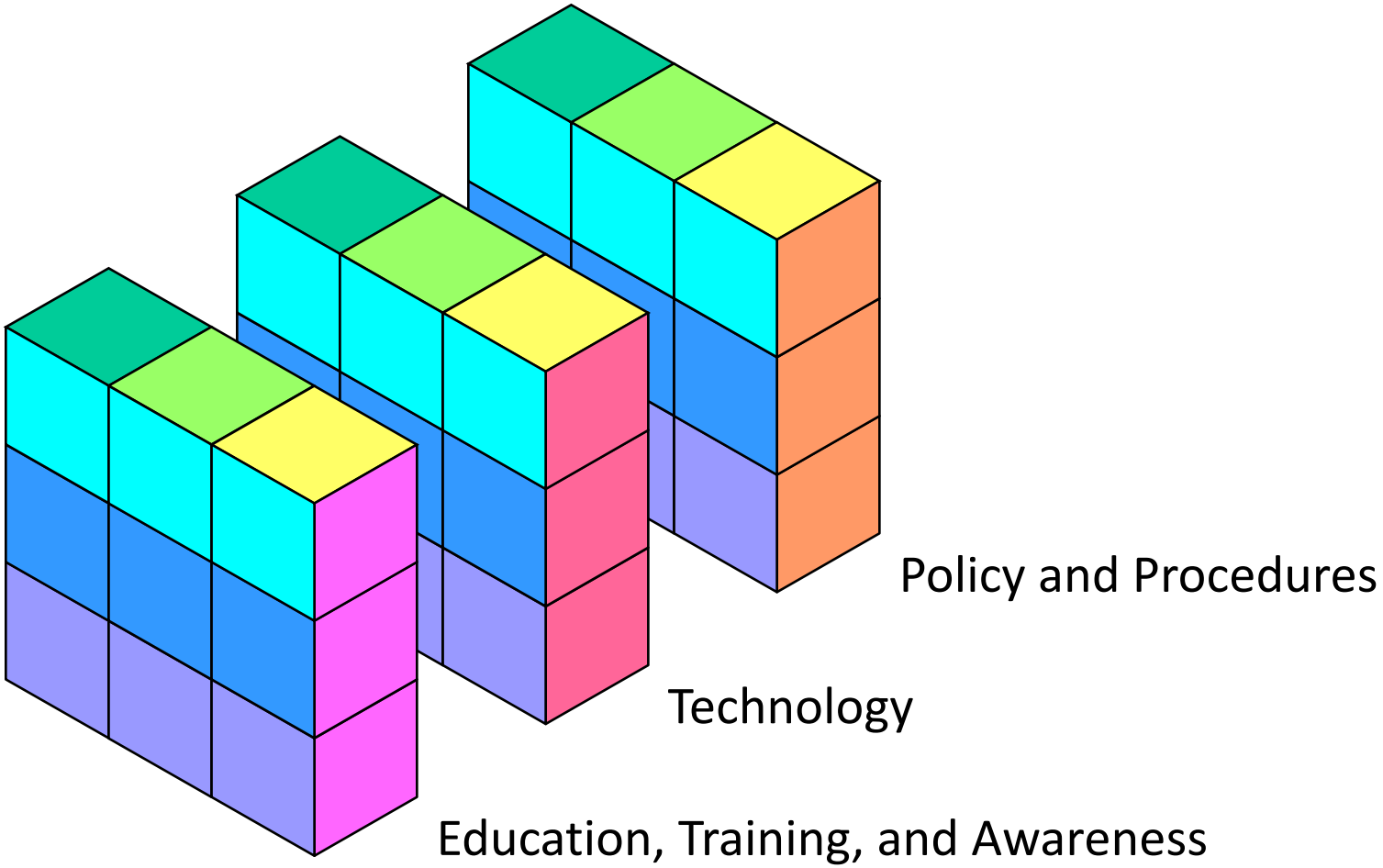
Availability



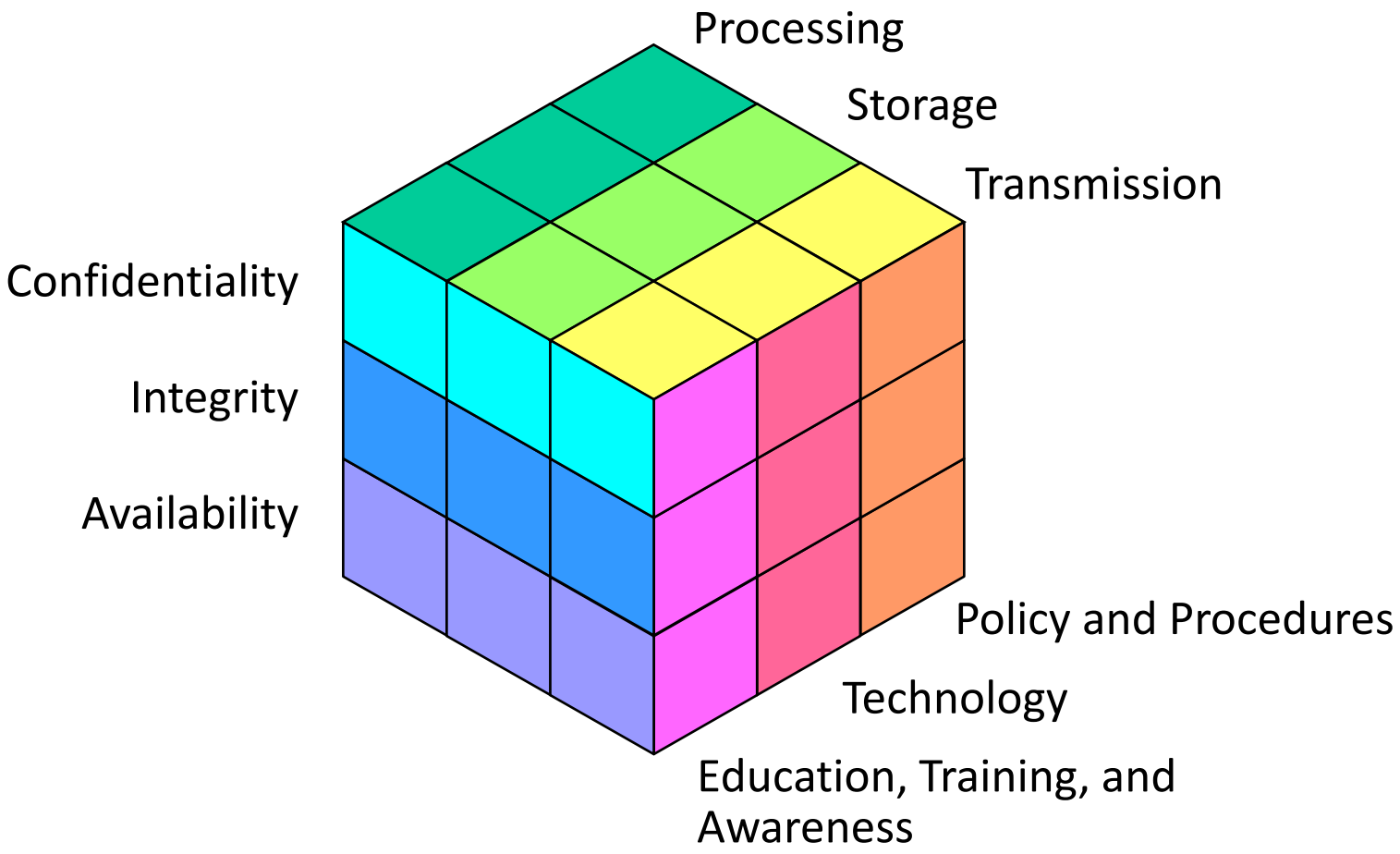
Information States



Security Measures



Information Security Model



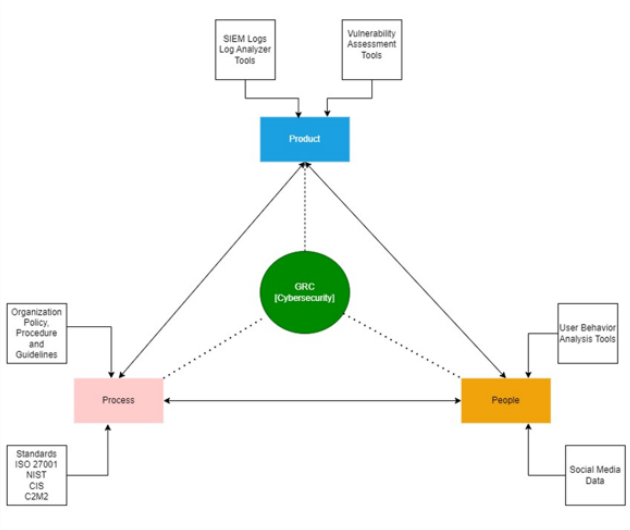
Information Security Life Cycle

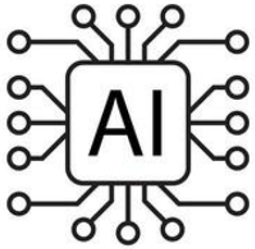
Security Responsibilities: WHO ??

- Information Security Management Committee
- Senior Managements
- Information Security Manager/CISO and Department
- Incident Response Team
- Business Continuity Team
- IT, Legal/Compliance, HR, Risk and other departments
- Audit Committee
- Last but not least, **YOU..!!**

My Endeavor Model

GRC Cybersecurity Engine



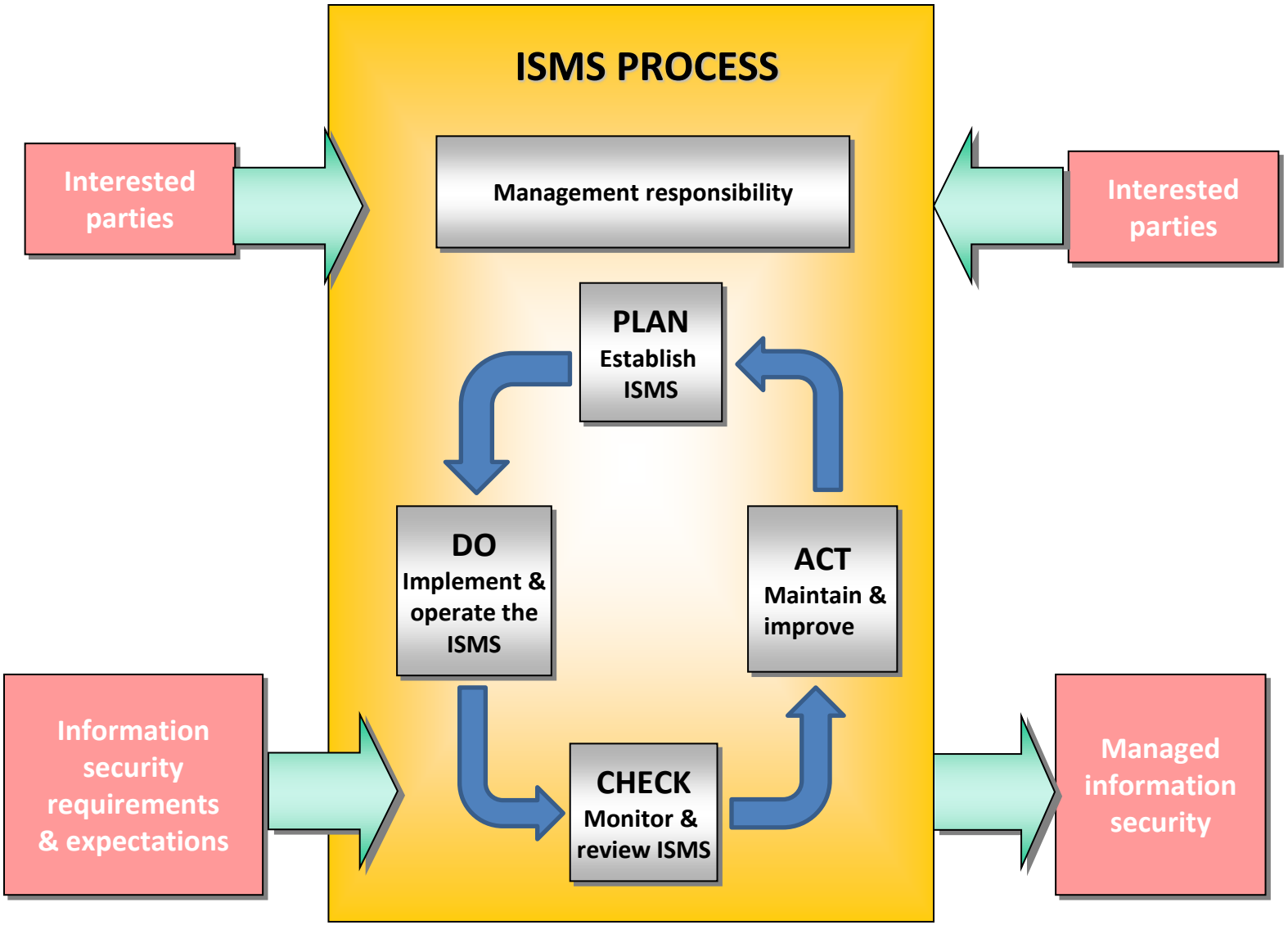


Towards Adaptive, Integrated, and Resilient Cybersecurity

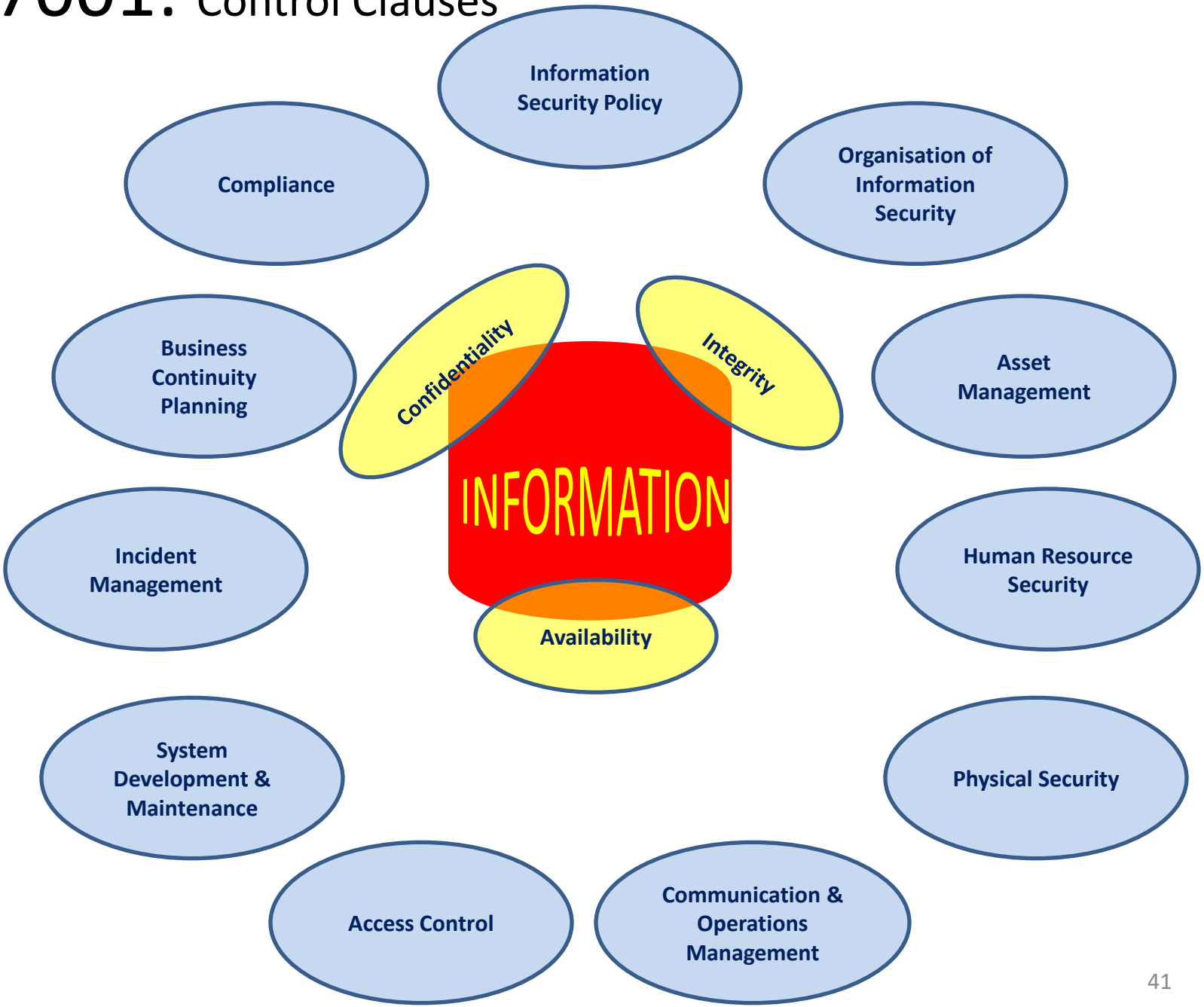
June 2024

Information Security Management Systems (ISMS)

ISO 27001: PDCA



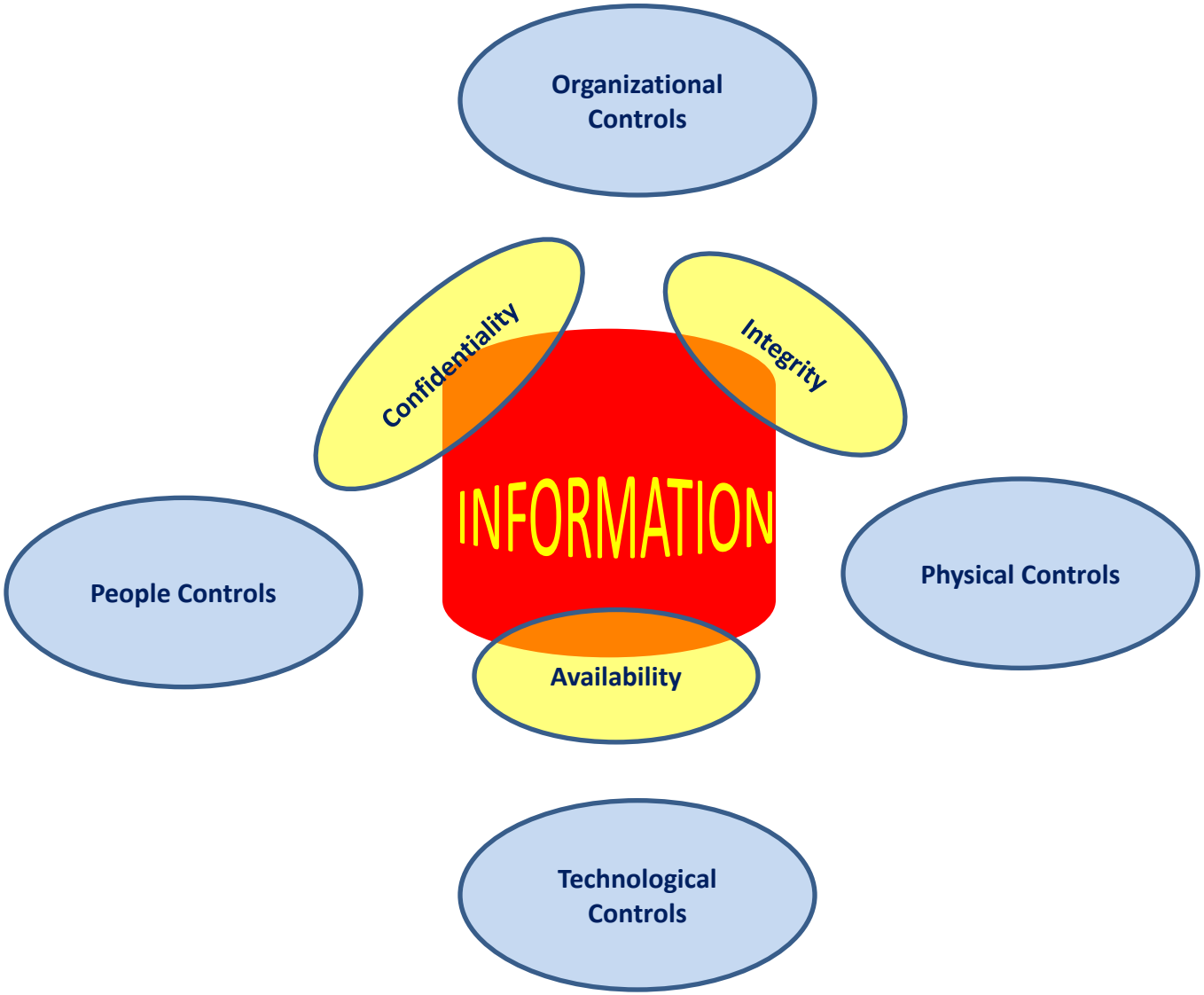
ISO 27001: Control Clauses



ISO 27001:2013 Control Clauses

114 Controls Clauses

ISO 27001:2022 Controls



ISO 27001:2022 Controls

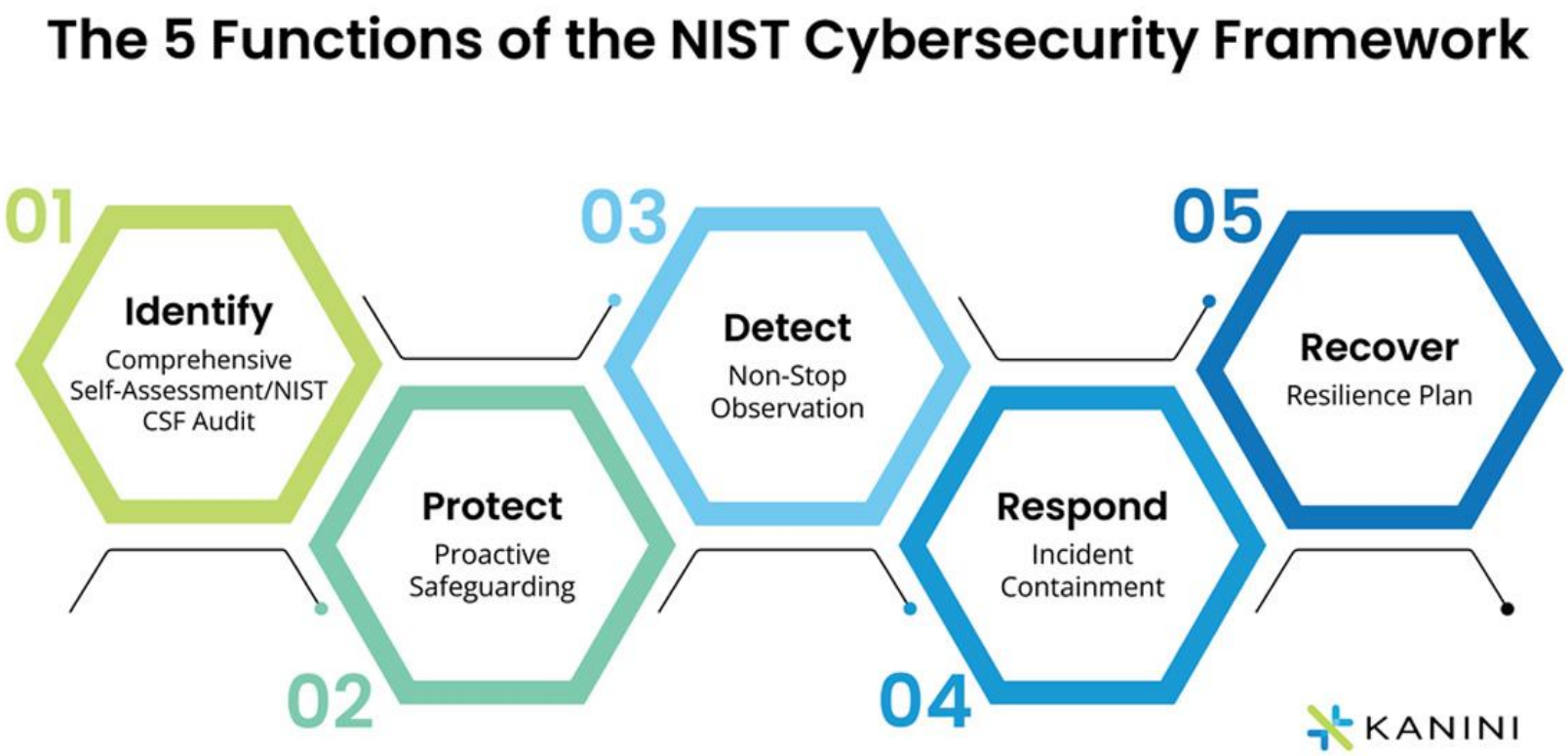
93 Controls
11 New Controls
58 Controls have been Reviewed and Revised
24 Controls are a Combination of 2,3 or More

ISO 27001:2022 New Controls

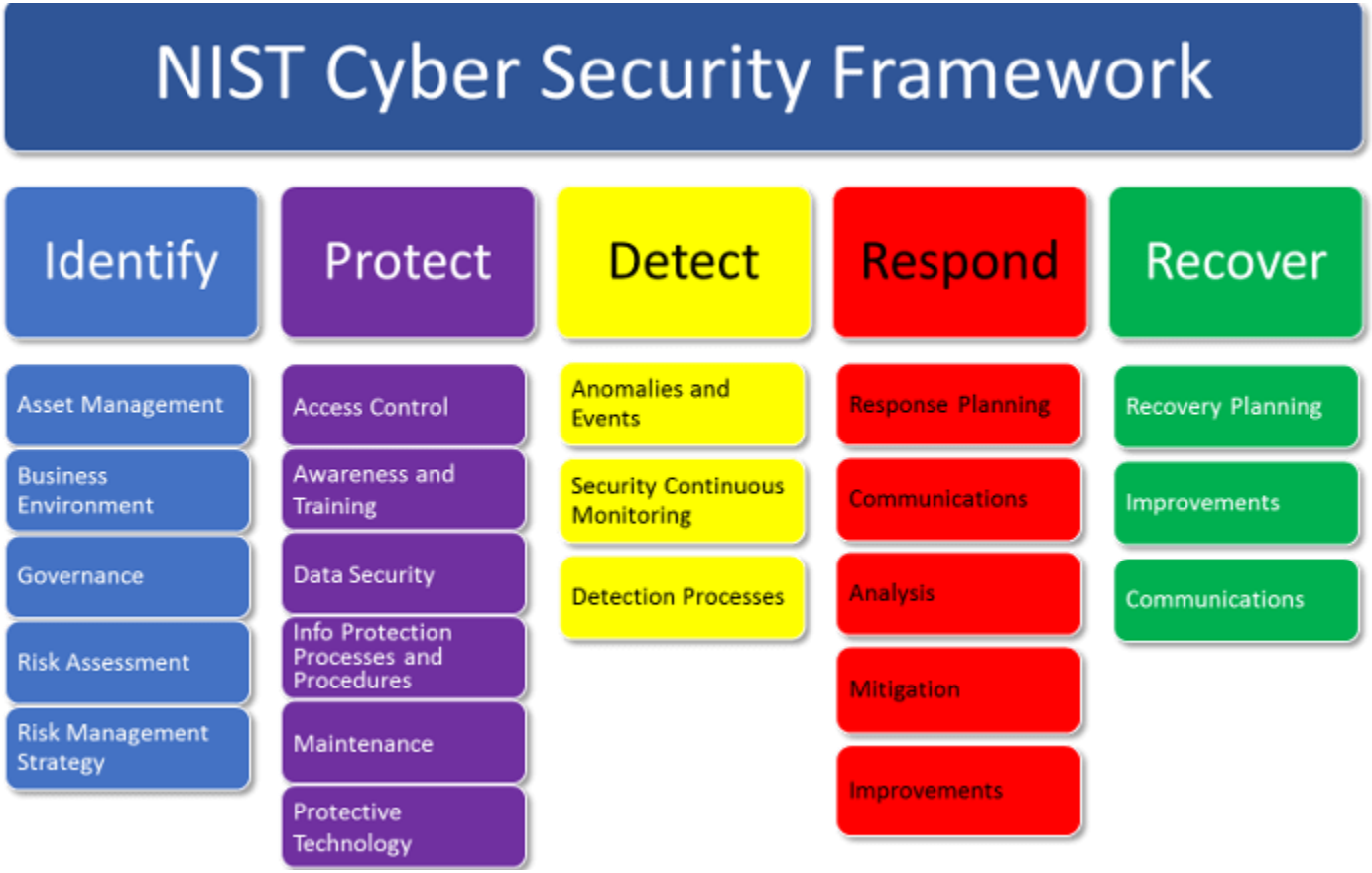
A.5	Organizational Control	5.7	Threat intelligence	NEW
A.5	Organizational Control	5.23	Information security for use of cloud services	NEW
A.5	Organizational Control	5.30	ICT readiness for business continuity	NEW
A.7	Physical Controls	7.4	Physical security monitoring	NEW
A.8	Technical Controls	8.9	Configuration management	NEW
A.8	Technical Controls	8.10	Information deletion	NEW
A.8	Technical Controls	8.11	Data masking	NEW
A.8	Technical Controls	8.12	Data leakage prevention	NEW
A.8	Technical Controls	8.16	Monitoring activities	NEW
A.8	Technical Controls	8.23	Web filtering	NEW
A.8	Technical Controls	8.28	Secure coding	NEW

NIST Cyber Security Framework

NIST Cyber Security Framework



NIST Cyber Security Framework



Cybersecurity Framework Components

Cybersecurity outcomes and informative references

Enables communication of cyber risk across an organization

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

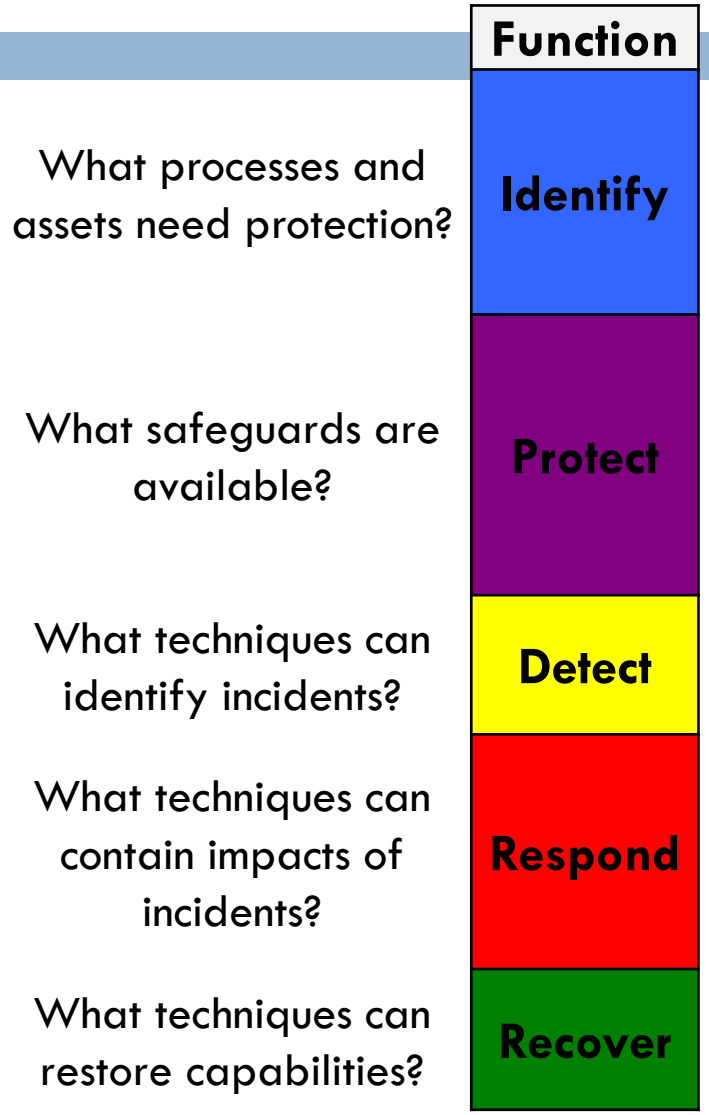
Aligns industry standards and best practices to the Framework Core in an implementation scenario
Supports prioritization and measurement while factoring in business needs

Implementation Tiers

	1 Partial	2 Risk Informed	3 Repeatable	4 Adaptive
Risk Management Process	The functionality and repeatability of cybersecurity risk management			
Integrated Risk Management Program	The extent to which cybersecurity is considered in broader risk management decisions			
External Participation	The degree to which the organization: • **monitors and manages supply chain risk**[1.1] • benefits by sharing or receiving information from outside parties			

Core

A Catalog of Cybersecurity Outcomes

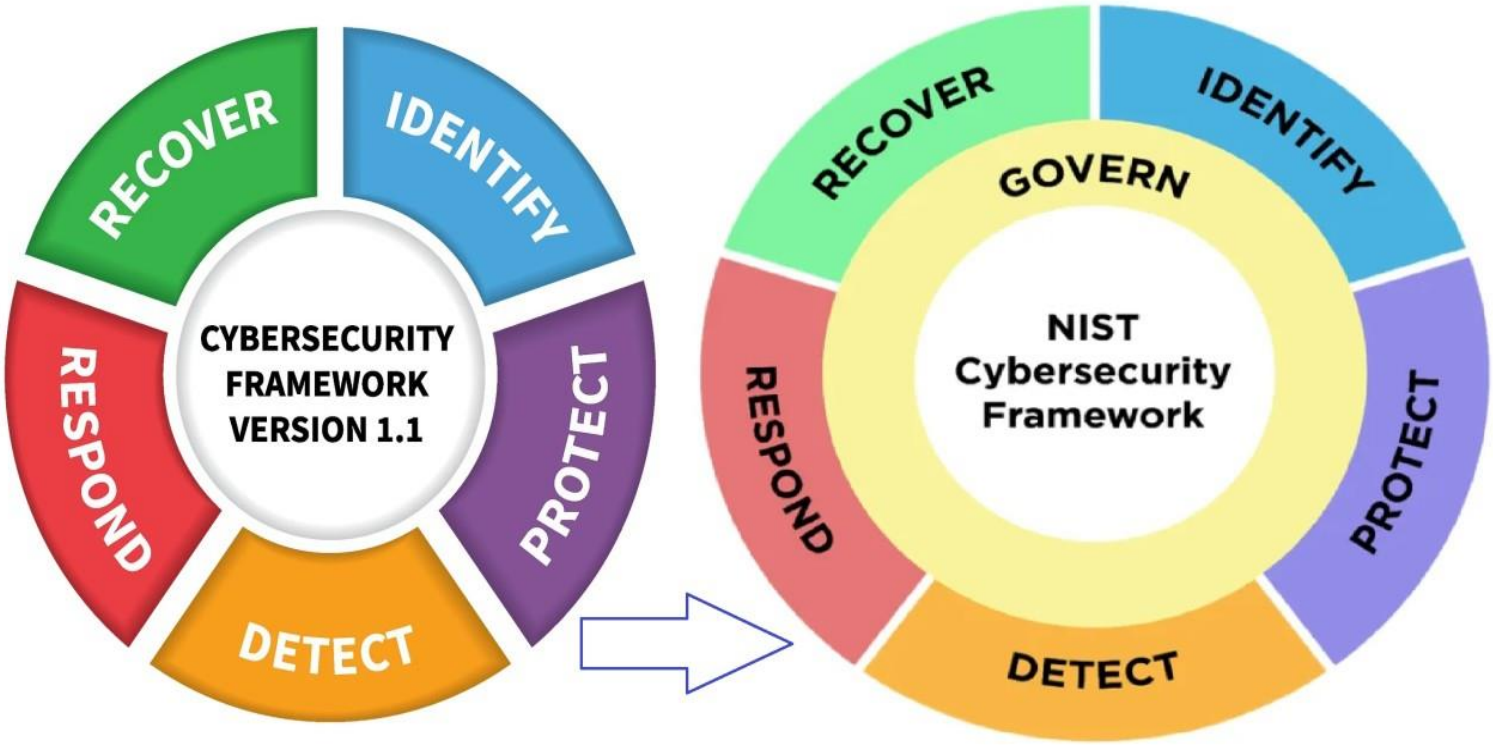


- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

Core

A Catalog of Cybersecurity Outcomes

	Function	Category
What processes and assets need protection?	**Identify**	Asset Management
		Business Environment
		Governance
		Risk Assessment
		Risk Management Strategy
		Supply Chain Risk Management[1.1]
What safeguards are available?	**Protect**	**Identity Management, Authentication and Access Control**[1.1]
		Awareness and Training
		Data Security
		Information Protection Processes & Procedures
		Maintenance
		Protective Technology
What techniques can identify incidents?	**Detect**	Anomalies and Events
		Security Continuous Monitoring
		Detection Processes
What techniques can contain impacts of incidents?	**Respond**	Response Planning
		Communications
		Analysis
		Mitigation
		Improvements
What techniques can restore capabilities?	**Recover**	Recovery Planning
		Improvements
		Communications



NIST Cyber Security Version 1.1 to Version 2.0

Thank You

Kumar Pudashine
kumar.pudashine@ieee.org