



Critical Telecom Infrastructure & Telecom Cyber Security

27th September 2024



Thoughts from **Alok Gupta**
Co-Chair Cyber Security Committee, BIF
Founder & CEO Pyramid Cyber Security &
Forensic

Alok Gupta

- Experience: 35 years in the Information and Communications Technology (ICT) industry
<https://www.linkedin.com/in/alokgupta65/>
- Serial Entrepreneur , Founder & CEO, Pyramid Cyber Security & Forensic, a boutique Digital Forensic and specialised Information Security solution and services provider
- Past member of the National Committee on Information Technology and current member of the regional committee on Digital Transformation for Confederation of Indian Industries (CII)
- Advised several Enterprises and Government agencies leverage use of ICT and Information Security to compete and grow in the global economy.
- Member Board of Governors Birla Institute of Management Technology
- Faculty FAFD ICAI
- Co-Chair Cyber Security Committee of Broadband India Forum
- Writes Columns, frequently quoted in IT, Security & Forensic media , regularly speaks at several events, workshops, seminars and forums in India and Internationally

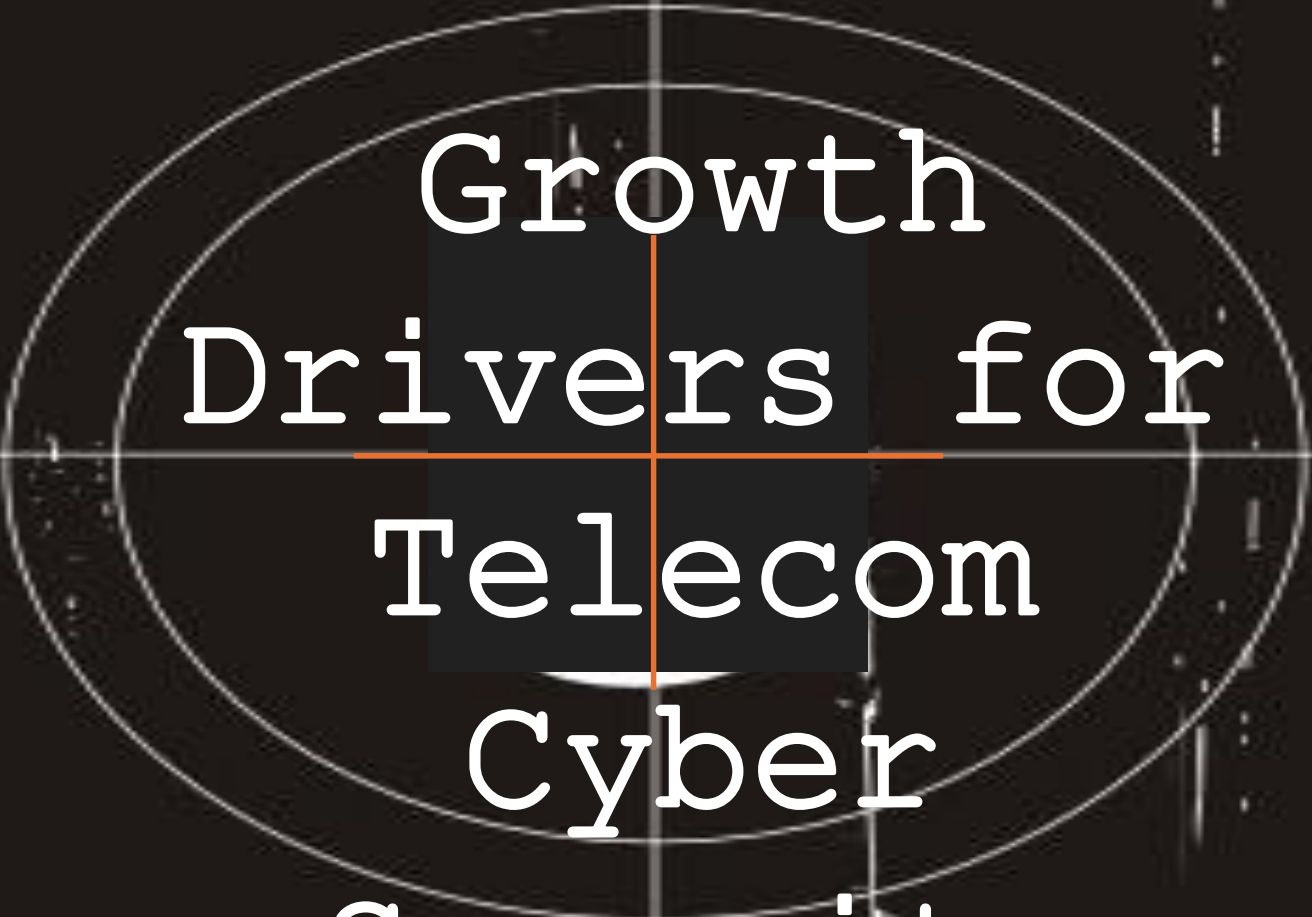


Session
Takeaway
S

Today we will address

- Growth Drivers for Cyber Security
- Cyber threats & Risk faced by Telecom Sector
- How to Prevent & Protect
- Zero Trust: Never Trust Always Verify





Growth
Drivers for
Telecom
Cyber
Security

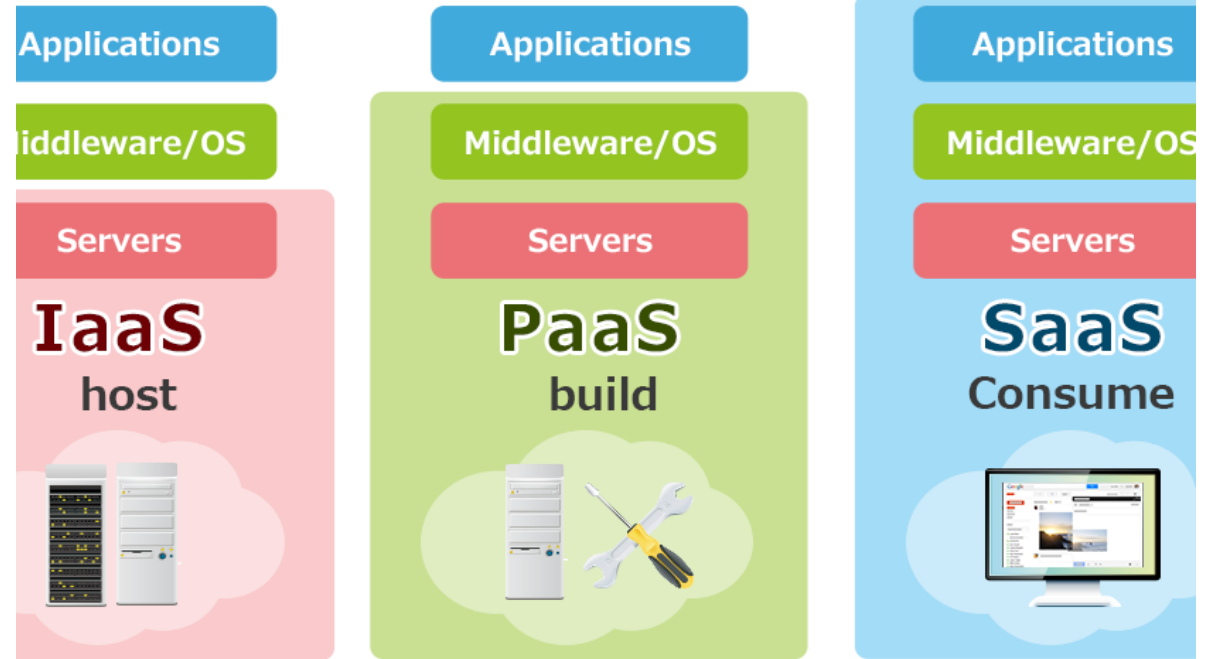
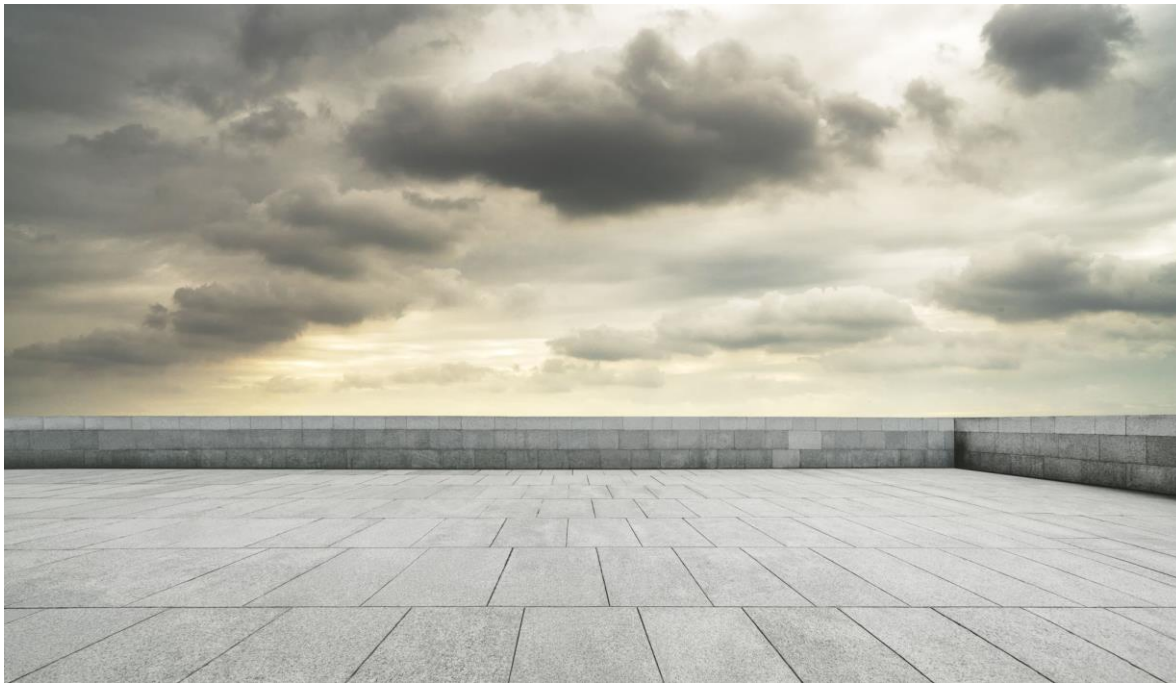
7+ Billion Mobile Phones in the
World

THE RISE OF MOBILE

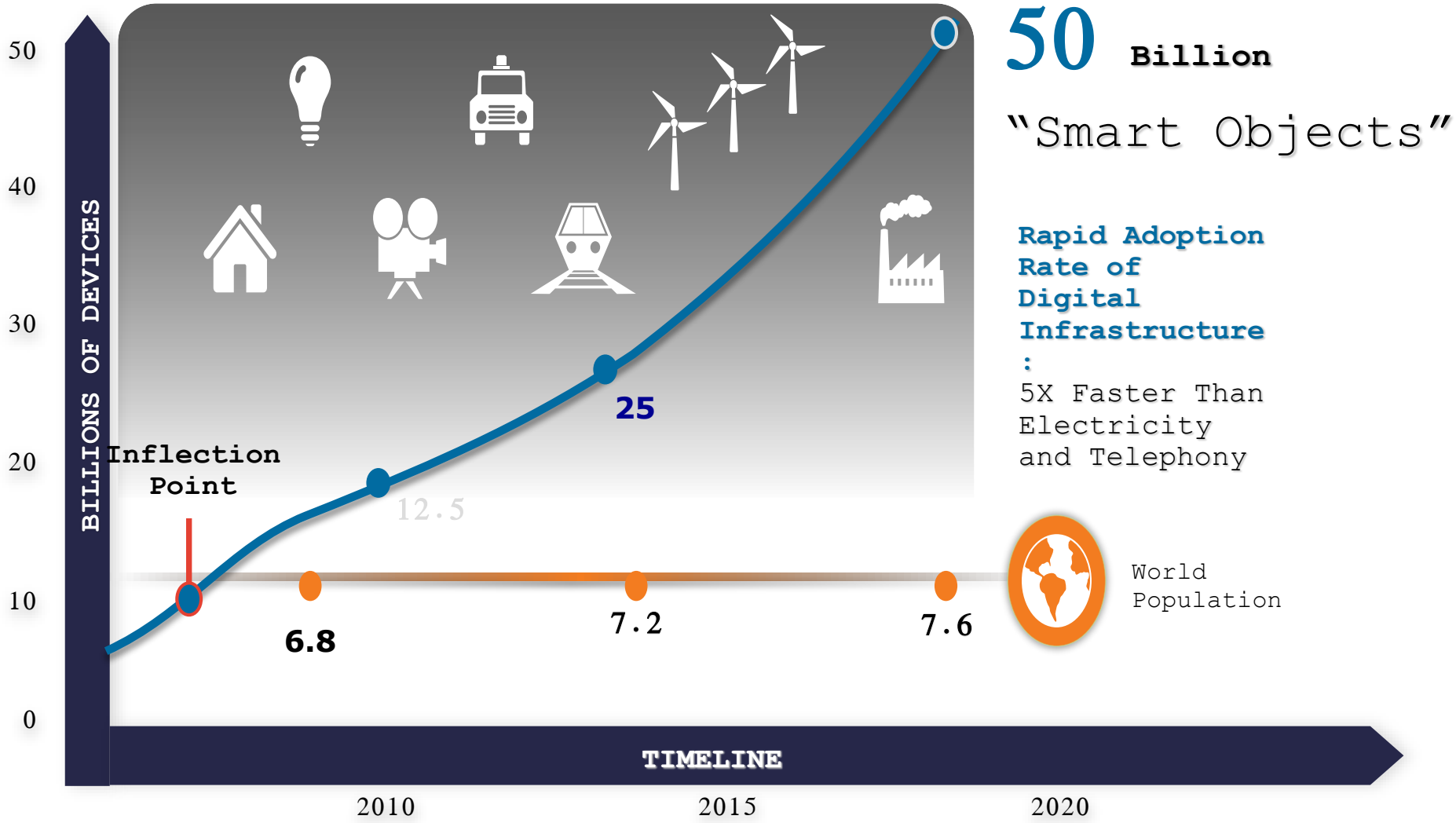


Rapid Cloud Adoption!

Cloud revenues poised to reach \$2 trillion by 2030 amid AI rollout



growing!



Social, Emails, Videos, Messaging, Calls

- Social media: On Twitter, 277,000 tweets are sent per minute.
- On Instagram, more than 216,000 new posts are made per minute.
- Email: Over 204 million emails are sent per minute.
- YouTube: 72 hours of videos are watched per minute.
- Google: 3.6 million searches are delivered per minute.
- Wikipedia: 600 new edits are published per minute.
- Calls: A minute of call can generate 740 kb of data.
- WhatsApp: Over 100 billion messages are sent to each other daily, with each chat averaging around 30 kb or less.





Cybercriminals are
exploiting everyone everyday

DPDP BILL

DEMYSTIFIED



Intent

Ensure that digital personal data processing is conducted lawfully, ethically, and with full transparency, while also promoting innovation and growth

Scope

The DPDP Bill applies to personal data, which is processed digitally, whether collected online or digitized offline



Geography

Within territory of India
-Extends to processing of India's digital personal data outside the Indian territory



Digital Personal Data



Digital data about an individual that can identify them. This includes identifiers like name, phone number, Aadhaar, PAN



Childrens Data

Data about an individual below the age of 18 that can identify them



Stakeholders

-Data Principal
-Data Fiduciary
-Significant Data Fiduciary
-Data Processor
-Data Protection Board of India

Grounds of processing Digital Personal Data

-By consent for legitimate use
-Lawful purpose



Rights of Data Principal

-Right to access
-Right to correction and erasure
-Right of grievance redressal
-Right to nominate



Duties of Data Principal

-Follow all laws
-Be impersonation
-Share complete & accurate details
-File false complaints
-Provide authentic information

Obligations of Data Fiduciary

-Give notice to data principal
-Obtain consent of data principal
-Data accuracy & completeness
-Security measures to prevent data breaches
-Notify of the data breach
-Delete data after purpose is fulfilled



Cross Border Data Processing & Transfer



The Bill permits the transfer of personal data outside India, except to countries restricted by the government through official notification

Data Breach Notification

Data Fiduciary or Data Processor must notify the Board and each affected Data Principal on the intimation of data breach



Enforcement

Data Protection Board is the regulatory authority with data processing and breaches with power to impose penalties



Penalty

Up to INR 250CR



Data privacy is the practice of keeping data safe and confidential, and preventing unauthorized access, theft, or loss. It's important for both individuals and businesses to protect their data, as data breaches can have serious consequences.



Cyber
Threats &
Risks faced
by Telecom
Sector

TOP TEN

Most worrisome risks for your company



Economic Societal Tech Geopolitical Environmental



Cyber threats faced by Telecom Sector

Telecom companies store a lot of sensitive data, making them an attractive target for cyberattacks.

Malware and ransomware: These attacks can disrupt services and affect many consumers

Social engineering and phishing: These attacks can compromise subscriber credentials or devices

DDoS attacks: These attacks can disrupt services

Cyber threats faced by Telecom Sector

Insider threats: Employees can mishandle sensitive information intentionally or through poor security habits.

Supply chain vulnerabilities: Hackers can target supply chains to gain access to customer data or disrupt operations

Internet of Things (IoT): The increasing use of IoT devices increases the number of potential attack surfaces

SYNful knock: This is a modified device firmware image that can replace the original operating system.

CYBER RISK

- Cyber risk is the possibility of financial loss, reputation damage, or disruption to an organization's operations due to failures in its information technology systems
- Hackers and Cyber Criminals are using novel methods and techniques to target remote workers and compromise business critical and sensitive corporate information

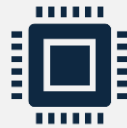
Some Recent Telecom Breaches and Attacks



BSNL data breach: In December 2023, a threat actor known as "Perell" published a dataset of sensitive information about BSNL's fiber and landline service users on a dark web forum. The dataset included email addresses, billing information, contact numbers, and more.



Tencent data breach: In August 2024, a hacker known as "Fenice" exposed the personal information of 1.4 billion Tencent user accounts. The leak included sensitive data such as emails, phone numbers, and QQ IDs.



AT&T experienced a metadata breach. AT&T also experienced a data breach in 2019 that was leaked in 2024

More Cases

SFR, Free, Bouygues, and Alphasud in France

Frontier Communications in the United States

Edpnet in Belgium

Triacom, Misto TV, Linktelecom, and KIM in Ukraine

Tangerine in Australia

Orange España in Spain

Kyivstar in Ukraine

Mint Mobile in the United States

Xfinity in the United States

INSIDERS

VS.

OUTSIDERS

WHAT'S THE GREATER CYBERSECURITY THREAT?

Malware Basics

- Malware, is a malicious software used or created to disrupt computer operation, gather sensitive information, or gain access to computer network and mobile systems.
- Malware can appear in the form of code, scripts, active content, and other software.



The Malware Museum

- Viruses
- Worms
- Trojans
- Spyware/Adware/Ransomware
- Bots / Robots / Agents
- Backdoor / Trapdoor
- Zombie
- Porn Diallers
- Key loggers
- Exploits
- Bug
- Rootkits



Phishing
and
Ransomware
Attacks are
a common
thing



Most Dangerous Hacker Groups

Fancy Bear (a.k.a. Sofacy, Pawn Storm) / Cozy Bear (a.k.a. CozyDuke, Office Monkeys)

- Russia, Influencing American Elections

Lazarus Group (a.k.a. DarkSeoul, Guardians of Peace)

- North Korea, Sony Pictures

Equation Group

- NSA, Iran's Nuclear

Comment Crew (a.k.a. APT1, Shanghai Group)

- People Liberation Army, Coke, RSA, Lockheed


Sandworm (a.k.a. Electrum),

- Russia, Attacking Critical Infrastructure

Distributed Denial-of-Service (DDoS)

A Distributed Denial-of-Service (DDoS) attack is a cybercrime that involves flooding a server with malicious traffic to prevent users from accessing online services. DDoS attacks can be launched from a single computer or from a botnet, which is a network of compromised devices





How to
prevent
and
Protect



The Importance of

Cybersecurity

Awareness

How much end-users know about the cyber security threats their networks face, the risks they introduce and mitigating security best practices to guide their behavior.

Cyber Hygiene

Cybersecurity best practices that an organization's security practitioners and users need to undertake similar to having personal hygiene practices to maintain your own health, cyber hygiene best practices help protect the health of your organization's network, assets & sensitive data



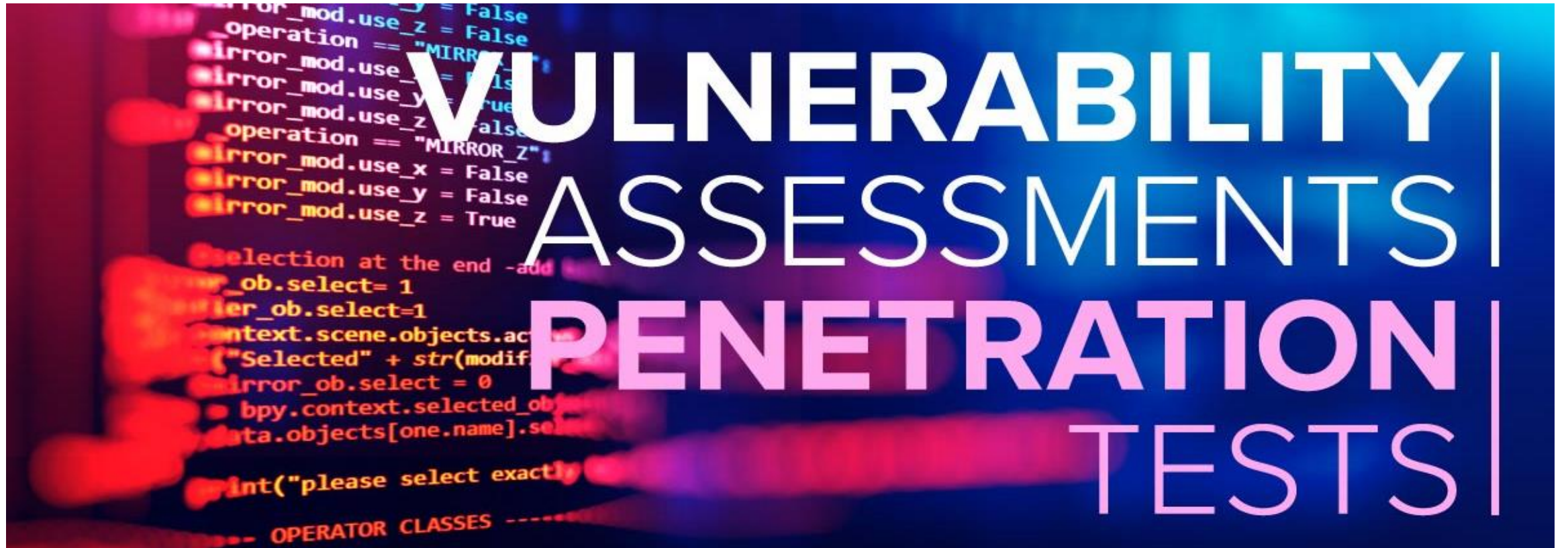
IT & Security Audit & Assessment

Get current system's internal control design and effectiveness against relevant standards, best practices and remote working including design, architecture, implementation, performance, efficiency, security protocols and IT governance.

Experts should be engaged to design and review incident response plan and check the organization's preparedness and readiness for a revised cyber insurance



Information
Security Audit



- Vulnerability Assessment scans should be performed on your network, applications, web infrastructure and end points to check critical and exploitable vulnerabilities.
- Thereafter Penetration tests exploitation is conducted to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat.

Red Team Exercise

Red Teaming is the process of using tactics, techniques, and procedures to emulate real-world adversaries to train and measure the effectiveness of the people, processes, and technology used to defend organizations

TEAM EXER

Enable Multifactor Authentication:

Social engineering remote privileged employees will allow hackers to know and steal credentials allowing them to access business critical information as insiders.

Multifactor Authentication System allows remote employees to leverage convenient & flexible tokens for secondary authentication of all end points, trusted devices, VPN, on-premise and cloud applications, to prevent credential theft and unauthorized access while meeting the regulatory needs

Multifactor authentication



Time



Something
you have



Something
you are



Something
you know



Location



24x7 Continuous Monitoring & Threat Intelligence

- 24x7 Log & network monitoring correlated with threat feeds to not only meet the compliance requirements of continuous monitoring at the same time giving you instant alerts and intuitive dashboard for governance as well as remediation via Managed Security Services Platform



Secure Configuration Management

Misconfigurations can lead to breaches and cyber incidents

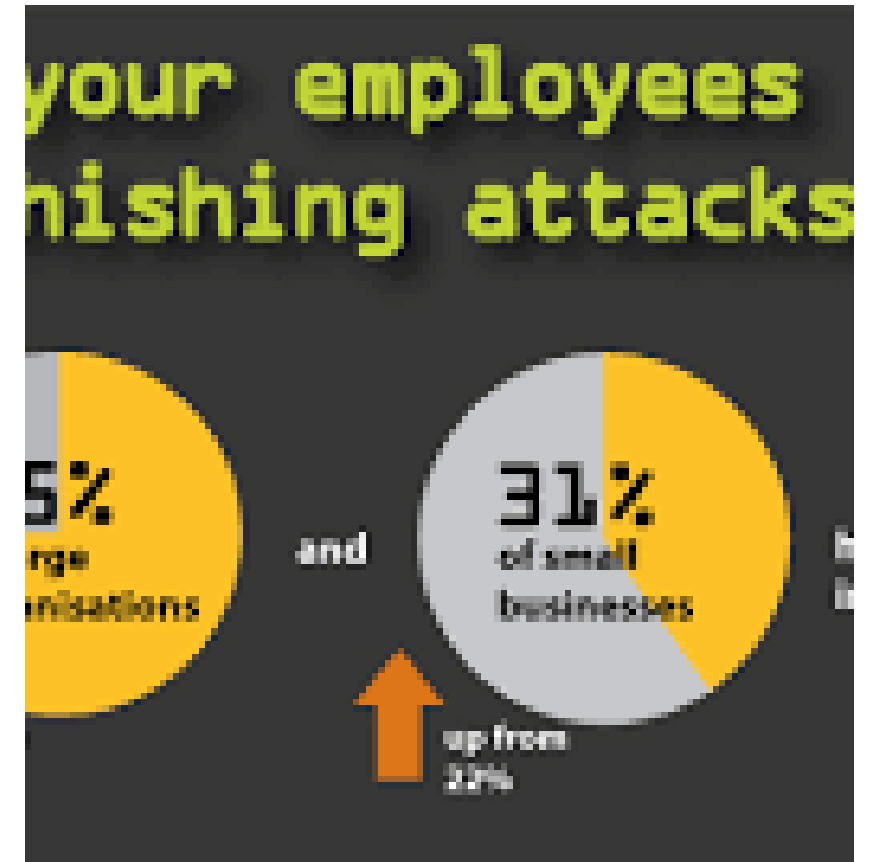
Compliance requires organizations to continuously check and remediate configuration issues in physical servers and VM's and provide audit-ready reports

Continuously and comprehensively identify and automatic remediation



Phishing Campaign Assessment

- Sophisticated threat actors mostly target senior leadership, privileged users, and those with payment authority.
- Very convincing campaigns and phishing attacks are launched to lure such users.
- Launch scenario based simulated campaigns for phishing assessment and employee awareness



Ensure Compliance to Data Privacy

Manage

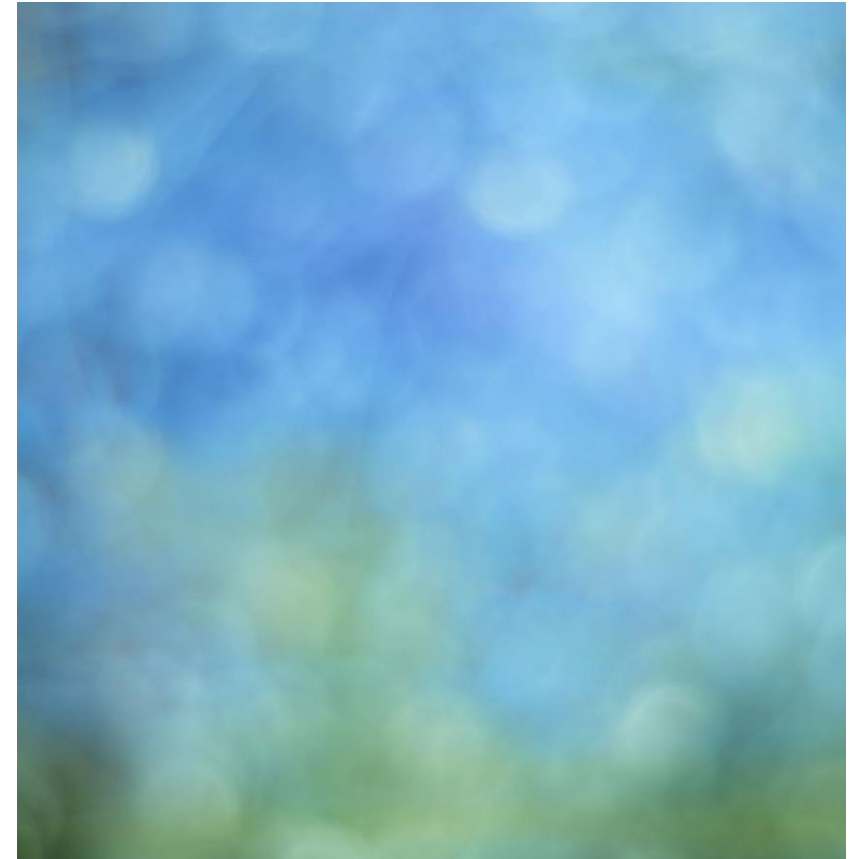
Manage access to sensitive and regulated data

Follow

Follow proper compliance requirements

Monitor
and
detect

Monitor and detect suspicious behavior on sensitive data



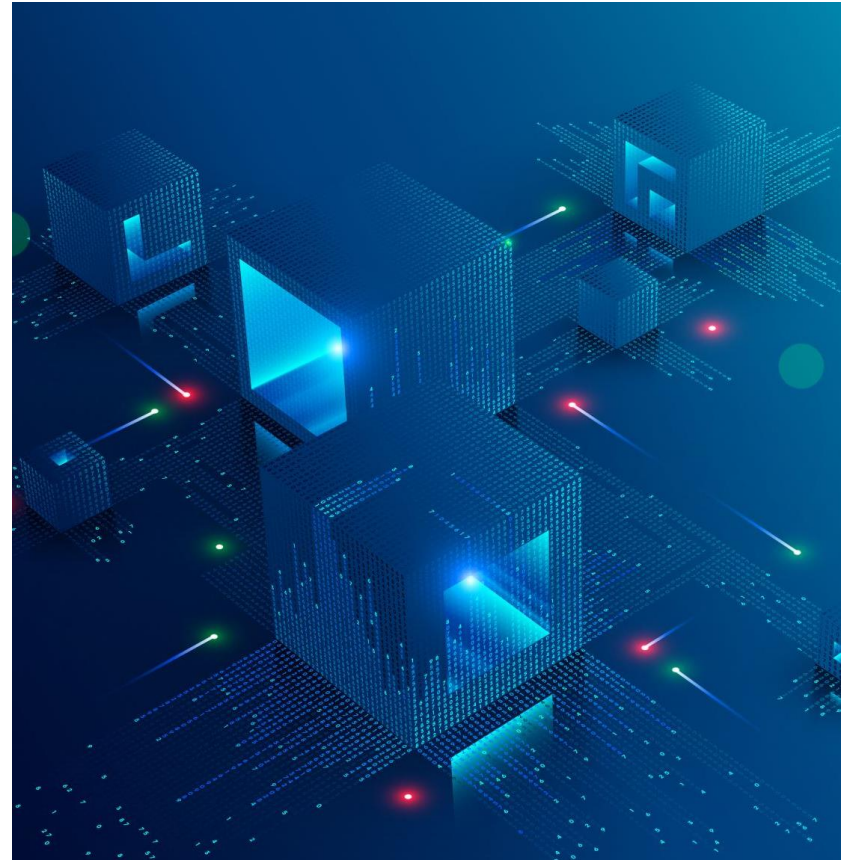
Worth it?

- Cyber insurance help businesses hedge against the potentially devastating effects of cybercrimes such as malware, ransomware, distributed denial-of-service (DDoS) attacks, or any other method used to compromise a network and sensitive data



Cyber Security Essentials

- Prediction, prevention, detection, resolution & protection from cyber attacks, breaches and threats
 - Design & Architecture (Zero Trust)
 - Audit & Assessment
 - VA-PT
 - Policy & Process
 - Compliance, Adoption of Standards
 - Data Leak prevention
 - Information Rights Management
 - Multifactor Authentication
 - Continuous Configuration Management
 - Security Information Event Management (SIEM)
 - Threat Intelligence & Security Analytics
 - Managed Security Service

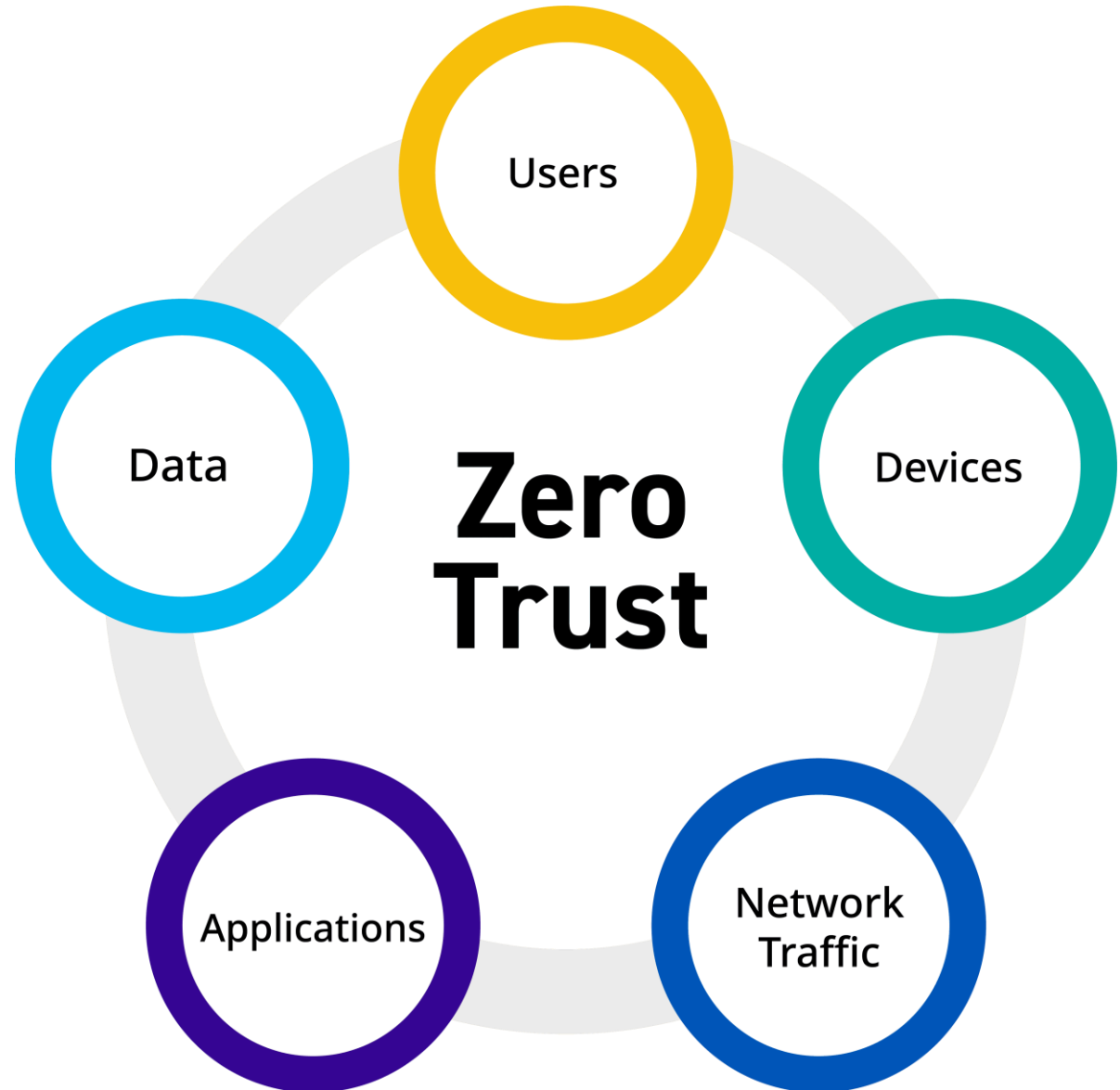


The image features a dark, textured background with a central graphic. The graphic consists of two concentric white circles. A dark gray square is centered within the inner circle. A thin orange vertical line and a thin orange horizontal line intersect at the center of the square, forming a crosshair. The text "Zero Trust" is written in a white, monospaced font across the center of the square.

Zero Trust

Zero Trust

Zero trust is a cybersecurity strategy that assumes no entity should be trusted by default. It's based on the principle of "**never trust, always verify**" and aims to prevent unauthorized access to data and services



Zero trust is a holistic approach

Define the attack surface

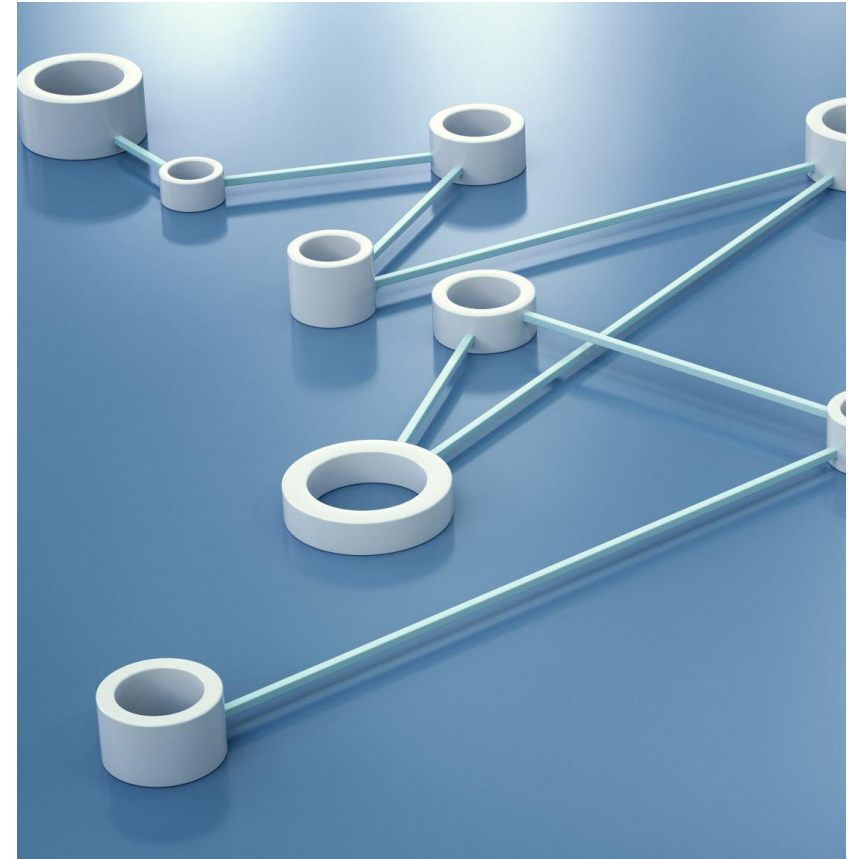
- Identify your organization's most critical assets, data, applications, and services (DAAS). This helps you prioritize where to start and create security policies.

Implement least privilege

- Grant users only the minimum access permissions they need to prevent exposure to sensitive areas.

Deploy multi-factor authentication (MFA)

- Require additional factors to prove a user's identity when accessing a network, application, or database.



Zero trust is a holistic approach

Develop a strong device identity

- Create a unique device identity that's attached to the device, not the user.

Conduct monitoring and auditing

- Review user activity across your network to identify suspicious activity in real time.

Don't trust your local network

- Apply the zero-trust framework to your internal network, assuming that no channel is completely secure.

Invest time and resources

- Implementing zero trust may require significant time, human resources, and financial resources.



Did Israel Infiltrate Lebanese Networks?

- Israel has been sending text messages, recordings, and hacking radio networks to warn Lebanese citizens to evacuate certain areas in the country, likely due to an imminent full-scale strike. Following these warnings, massive bombings in southern and eastern Lebanon
- They have details of people – cellphone numbers, locations. ... Is it because of data leaks or because Israel has hacked into Lebanon's telecoms infrastructure?





Thank You!

Alok Gupta,
Founder & CEO
Pyramid Cyber Security & Forensic
alok.gupta@pyramidcyber.com
9999189650



Questions?

Information Security

