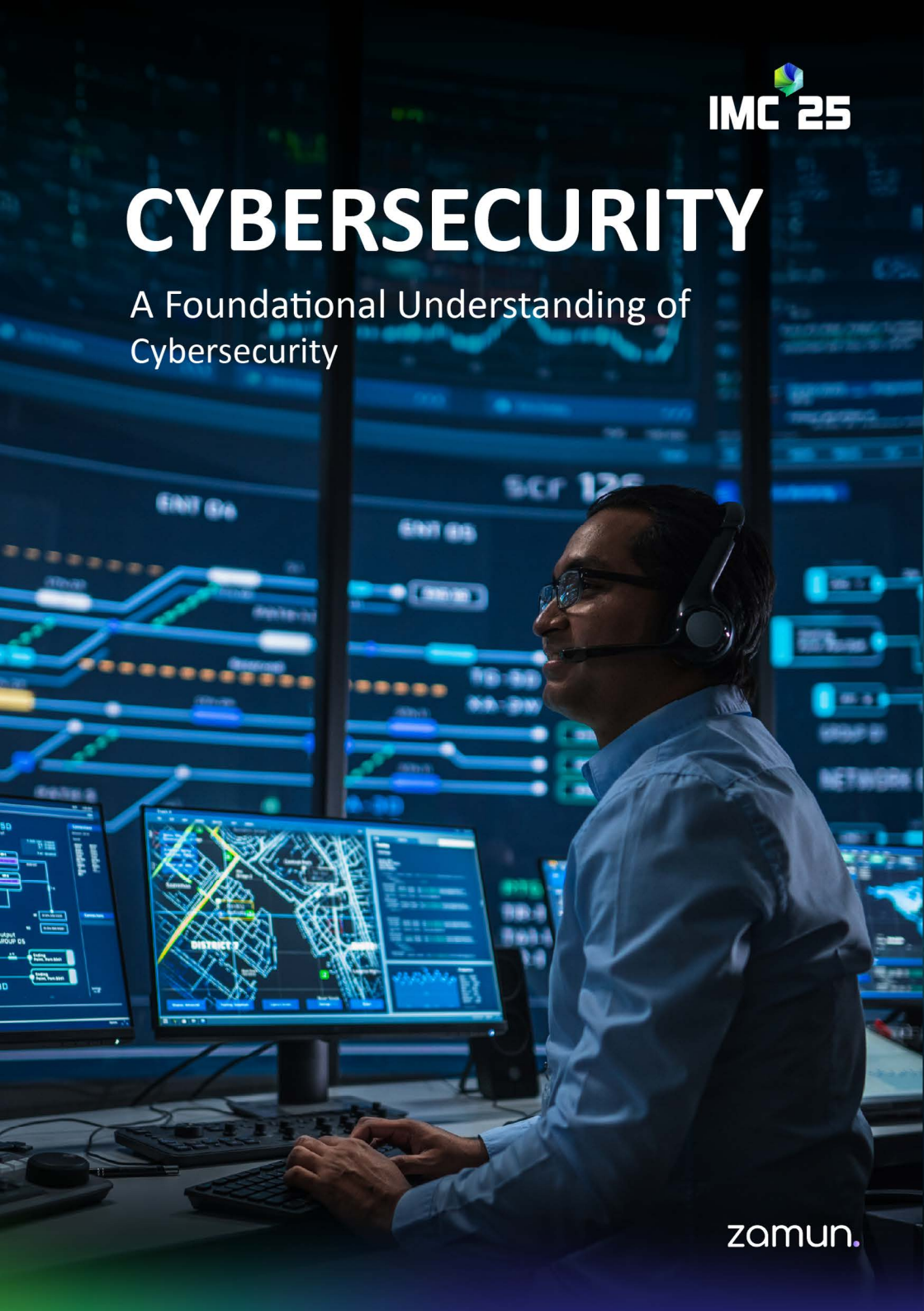
IMC 25

CYBERSECURITY

A Foundational Understanding of Cybersecurity



zamun.

Content

Dear Leaders

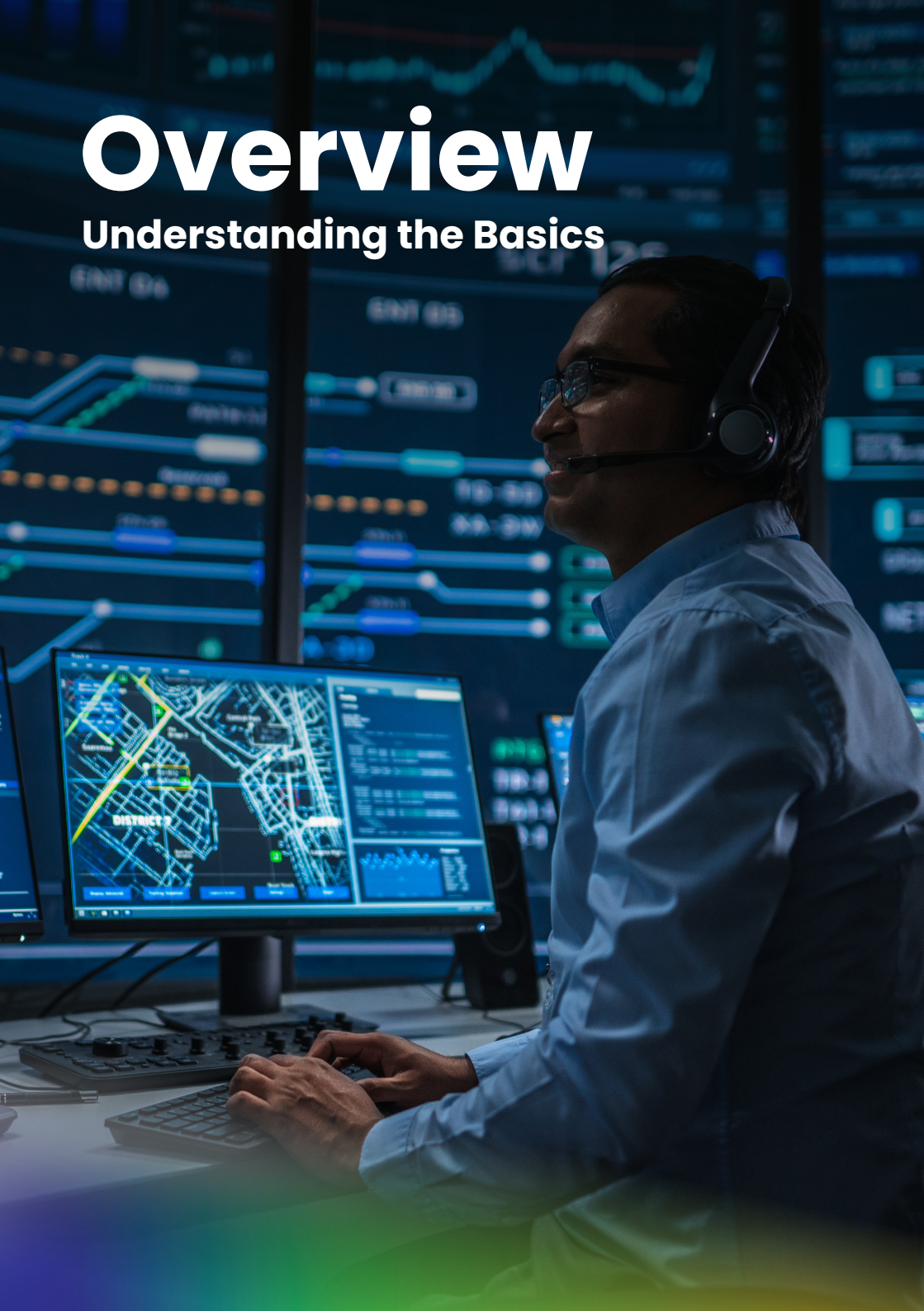
In a world defined by connection and speed, our reliance on digital infrastructure has never been greater—nor has the danger. Cybersecurity is no longer an IT niche; it is the fundamental currency of global trust and commerce.

This book is your essential guide to understanding this high-stakes domain. We journey from the multi-billion-dollar market dynamics and the tightening grip of global data regulations to the raw reality of the modern threat landscape, where ransomware gangs and advanced nation-state actors pose a constant, evolving risk. We explore the innovative defenses emerging at the network edge and in the cloud, dissecting the shift towards agile, as-a-Service business models.

Ultimately, this is a story of foresight. By examining the current battlefront, we prepare you for the inevitable future, one where autonomous AI security and quantum-safe protocols become the necessary standard for survival. Read this to move beyond defense—read this to truly master resilience.

Overview

Understanding the Basics



Defining Cybersecurity

CIA Triad, Zero-Trust, and Cyber

Resilience

Cybersecurity in 2025 goes beyond defense to resilience, embracing proactive measures to anticipate and mitigate threats

Core Concepts & Definitions

CIA Triad

- Confidentiality: Ensuring data is accessed only by authorized individuals.
- Integrity: Maintaining accurate, trustworthy data by preventing unauthorized modifications.
- Availability: Guaranteeing reliable access to information systems.

Zero-Trust Framework

- Assumes continuous verification of all users, devices, and network requests, even inside trusted zones.
- 75% of enterprises will implement a zero-trust architecture by 2026, up from 35% in 2022.

Cyber Resilience

- The capacity of organizations to anticipate, withstand, and recover from cyber disruptions.
- Companies adopting resilience frameworks reduced breach recovery time by 50% compared to traditional approaches.

Adoption Statistics

Concept	Adoption Rate (2022)	Projected Adoption (2026)
Zero-Trust	35%	75%
Cyber Resilience	40%	85%

Source: optiv.com

Step 1

Assess and Recommend

Define the protect surface by:

- Conducting a baseline assessment
- Subsequent check-ins to determine organizational posture

Palo Alto Networks Products

- Next-Generation Firewall
- VM-Series
- Cortex XDR
- Cortex Xpanse
- Prisma Cloud

72%

of companies are **prioritizing the adoption of a Zero Trust model**[1]

Step 2

Remediate and Build

Once the assessments are complete, it's important to remediate identified gaps by executing on a maturity roadmap.

Palo Alto Networks Products

- Next-Generation Firewall
- VM-Series
- Cortex XDR
- Cortex XDR Prevent
- Cortex Data Lake
- GlobalProtect
- Prisma Access
- Prisma Cloud
- Cortex XSOAR

99%

of companies who have adopted Zero Trust say it's **improved their companies cybersecurity**[2]

Step 3

Transformation Execution

Operate and continue to enhance Zero Trust capabilities through creation of Zero Trust policies and active monitoring.

Palo Alto Networks Products

- Panorama
- WildFire
- Threat Prevention
- URL Filtering
- DNS Service
- Prisma SaaS
- Prisma Cloud
- Threat Intelligence Management
- Cortex XSOAR
- Cortex Data Lake
- Cortex XDR
- Cortex XSIAM

72%

of companies say the top reason for Zero Trust adoption is to strengthen data security, followed by need to **improve identity and access management**[2]

Sources:

1 - Cybersecurity Insiders, VPN Risk Report, 2021

Evolution

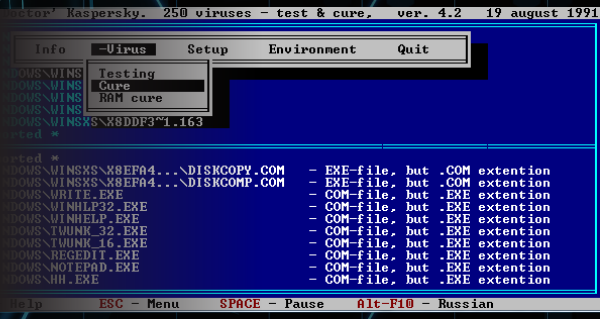
From Antivirus to AI-Driven Security Operations

Historical E volution Overview:

01.

1990–2000

Basic antivirus, firewall installations; reactive defenses dominated.



02.

2001–2015:

Rise of IDS/IPS, early SIEM systems; shift towards proactive threat detection.

03.

2016–2025:

Dominance of AI and machine learning, SIEM/SOAR integration, predictive analytics, and automated response.

Transformational Milestones (2025)

- AI-based security reduces average detection-to-containment time by 70%, from days to hours.
- Over 80% of enterprises employ security automation (SOAR) to manage routine incidents.
- Traditional signature-based antivirus solutions phased out in favor of behavioral AI detection.

Technology	Prevalence in 2010	Prevalence in 2025
Antivirus (Basic)	90%	<20%
AI-driven SIEM/SOAR	<10%	85%

Core Cybersecurity Tech Stack

AI, SIEM/SOAR, XDR, and Quantum-Safe Encryption

The cybersecurity tech stack of 2025 blends advanced threat detection and response with futuristic quantum-safe protection.

Essential Components

Artificial Intelligence (AI):

- AI-based threat detection identifies threats 80% faster than traditional methods.

SIEM/SOAR:

- Security Information and Event Management (SIEM) centralizes real-time monitoring.
- Security Orchestration Automation & Response (SOAR) automates repetitive response actions, increasing efficiency by 60%.

Extended Detection and Response (XDR):

- Provides holistic security visibility across endpoints, networks, and clouds.
- Reduces incident dwell time by 70%.

Quantum-Safe Encryption:

- Quantum-resistant algorithms protect against quantum computer-enabled decryption threats projected by 2030.

Comparative Efficiency

Technology	Incident Detection Efficiency	Reduction in Response Time
AI-driven SIEM	+75%	70%
SOAR Platforms	35%	60%
XDR Solutions	+85%	70%

Standards & Frameworks

Cybersecurity effectiveness relies on global standards and best practices providing unified governance and interoperability.

Major Frameworks & Standards

ISO/IEC 27001

- International standard governing information security management systems (ISMS); adopted by 70% of Fortune 500 companies.

NIST Cybersecurity Framework (CSF)

- Risk-based cybersecurity management widely adopted across critical infrastructure sectors, mandatory in U.S. federal agencies.

General Data Protection Regulation (GDPR)

- Enforced since 2018, driving privacy and data security reforms globally; fines up to 4% of annual turnover for non-compliance.

MITRE ATT&CK Framework

- Open repository for adversary tactics, techniques, procedures (TTPs); used by 60% of SOC teams globally for threat intelligence. 2025 Snapshot

Adoption and Compliance Trends

Standard	Global Adoption (2025)	Key Sector
ISO 27001	75%	Enterprise
SOAR Platforms NIST CSF	35%	60%
XDR Solutions	+85%	70%

Key Industry Verticals

BFSI, Healthcare, Telecom, Government & Defense

The cybersecurity tech stack of 2025 blends advanced threat detection and response with futuristic quantum-safe protection.

Vertical Threat Analysis (2025)

Sector	Cyberattack Share	Main Attack Vectors	Notable Recent Incidents
BFSI	30%	Ransomware, Phishing	SBI & ICICI phishing (2024)
Healthcare	25%	Ransomware, IoT vulnerabilities	AIIMS breach (2024)
Telecom	20%	Network DDoS, SIM swap	Jio SIM attack (2025)
Government	15%	APTs, Cyber espionage	NIC server breach (2024)

Sector-wise Cybersecurity Priorities

- BFSI: Real-time fraud detection, zero-trust architectures.
- Healthcare: Endpoint security for IoT devices, HIPAA/GDPR compliance.
- Telecom: 5G security implementation, automated defense mechanisms.
- Govt & Defense: AI-driven threat intelligence, secure infrastructure.

Hi Fellas!
Let us summarize our basics before moving forward. We started off with developing our basics on security, including Core Concepts & Definitions like the CIA Triad and Zero-Trust, which sets our stage for examining current Adoption Statistics. We then moved forward with the rapid Evolution from legacy antivirus to AI-driven systems, outlining the modern Core Cybersecurity Tech Stack (XDR, SOAR). And finally, we discussed governing Standards & Frameworks (NIST, ISO) and analyze specific threats across Key Industry Verticals.

With an insane touch upon the basics, Amigos.. Grab your coffees and gear up for our next set of understanding the current market trends.

Market Sizing and Trends

Global Cyberecurity Market

Size, Growth, and Key Regions

Cybersecurity investment and market dynamics are significantly influenced by increased digital transformation and regulatory pressures

Market Size and Growth (2025)

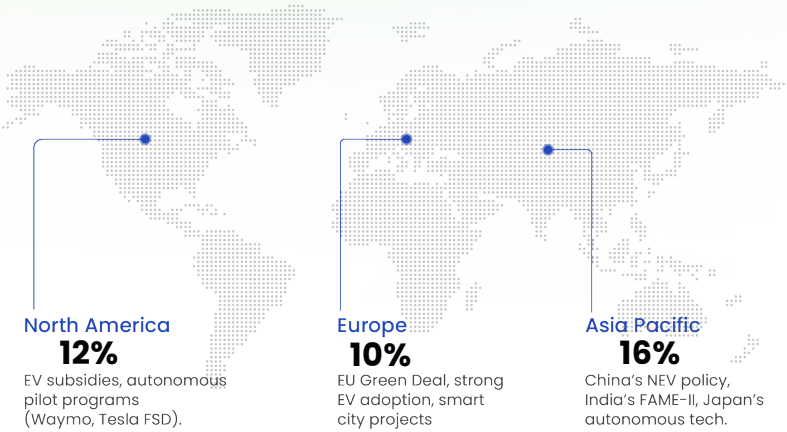
- Global cybersecurity market reaches USD 450 billion, growing at 12–14% CAGR (2022–2025).
- Managed Security Services (MSS) segment grows fastest, projected at 18% CAGR.
- Cloud security investments triple from USD 20 billion (2020) to USD 60 billion (2025).

Regional Market Breakdown (2025)

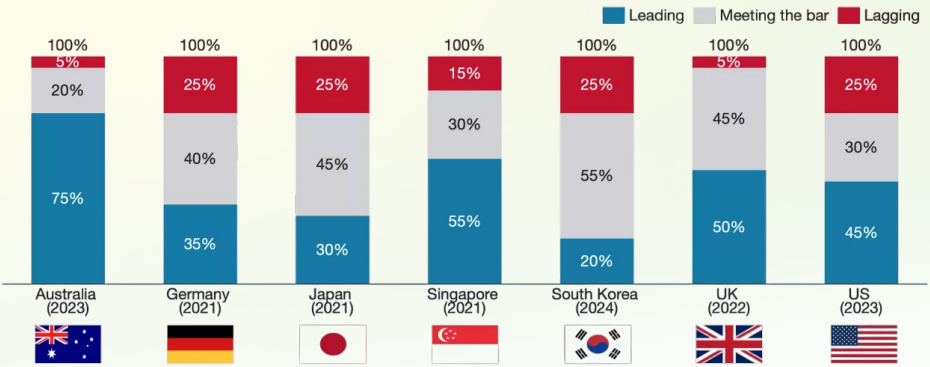
Region	Market Size	CAGR (2022–2025)
North America	USD 180 bn	12%
Asia-Pacific	USD 120 bn	16%
Europe	USD 100 bn	10%
Middle East & Africa	USD 30 bn	14%
Latin America	USD 20 bn	15%

Key Drivers of Market Growth

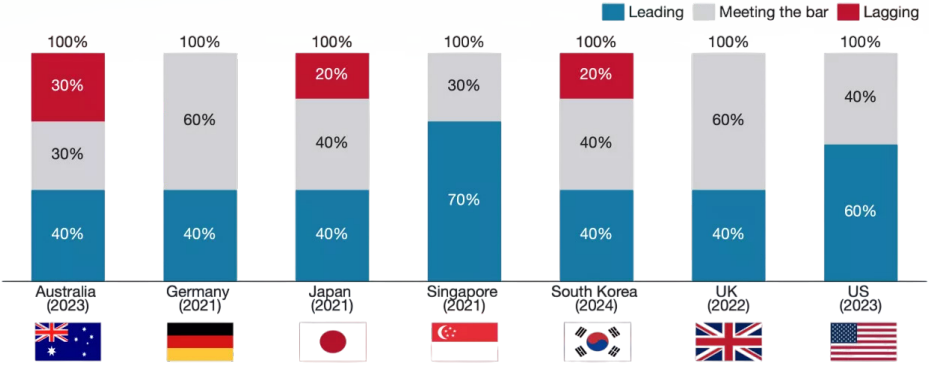
- Increased regulatory compliance requirements globally (e.g., GDPR, India's DPDP Act).
- Rising cyber threats amid geopolitical instability.
- Rapid cloud and IoT adoption creating new vulnerabilities.



This infographic shows the cybersecurity market projected to grow at 9.1% CAGR to $352B by 2030, driven by rising cyberattacks but constrained by talent shortages and high costs.



Cybersecurity investment and market dynamics are significantly influenced by increased digital transformation and regulatory pressures



Source: belfercenter.org

Country performances for Building Partnerships


Cybersecurity is the backbone of emerging technologies.

Cybersecurity in 2025

Global Snapshot of Threat Landscape

The global cybersecurity landscape in 2025 is marked by accelerated threats fueled by digital transformation and emerging technologies.

Key Threat Statistics

- Global cybercrime damage costs are projected to exceed USD 12 trillion by 2025, up from USD 8 trillion in 2022.
- Approximately 450 billion attempted breaches recorded annually, with successful breaches increasing by 20% year-on-year.
- Ransomware incidents surged 150% since 2020, with an average ransom demand crossing USD 5 million per incident.

Top Emerging Threats (2025)

Threat Category	Notable Example	Incident Growth (2022-2025)
Ransomware	Hive Ransomware	+150%
Supply Chain Attacks	SolarWinds-type Incidents	+300%
IoT Vulnerabilities	Smart City Exploits	+200%
AI-driven Attacks	Deepfake Social Engineering	+400%

Strategic Insights

- 90% of cyberattacks begin with human error, emphasizing the need for stronger training programs.
- Healthcare and financial sectors are the most targeted, comprising nearly 40% of total cyber incidents.
- Increased geopolitical tensions have raised state-sponsored cyber threats by 45% since 2020.

India's Cybersecurity Ecosystem

Policies, CERT-In Initiatives, and Regulations

Key Government Initiatives and Milestones

CERT-In (Indian Computer Emergency Response Team):

- Handles ~2 million cyber incidents annually (2025), a 43% increase since 2022.
- Released 1,500+ security advisories annually, impacting key sectors like BFSI, healthcare, telecom.

National Cybersecurity Policy 2020:

- Targets establishing 25 regional cybersecurity hubs by 2025, with projected cumulative investment reaching INR 10,000 crores.

Digital Personal Data Protection (DPDP) Act, 2023:

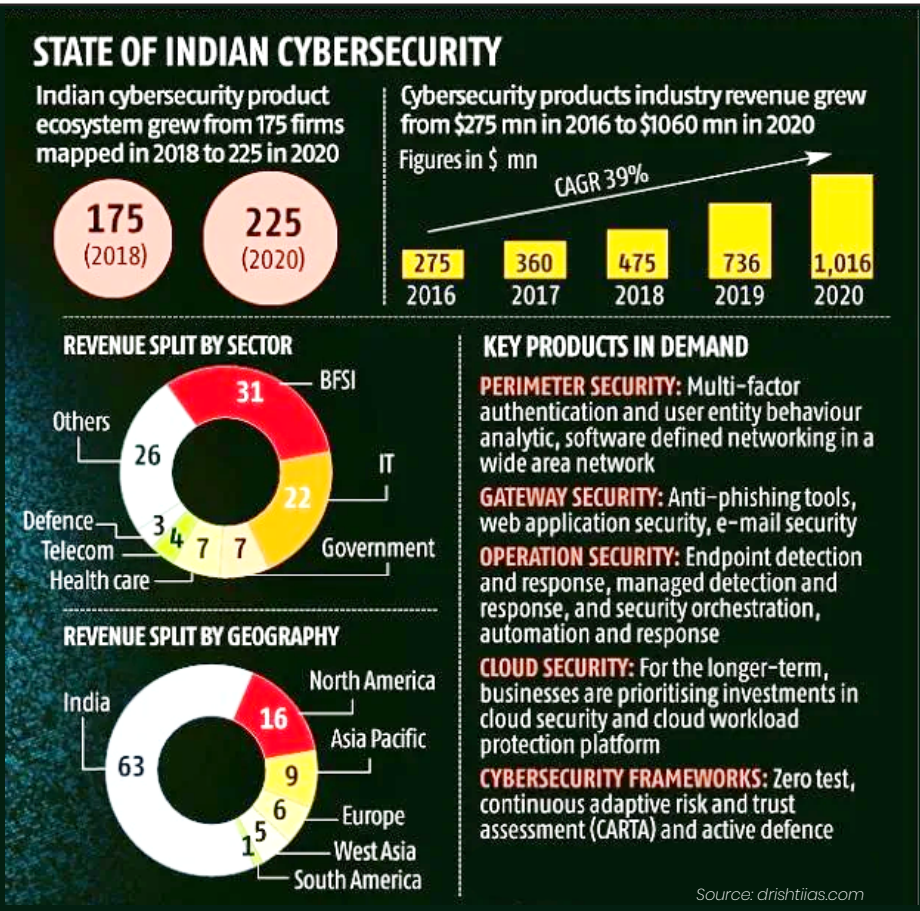
- Strict penalties (up to INR 250 crores) and regulatory oversight on data processing.

Regulatory Landscape Overview (2025)

Regulation	Focus Area	Adoption/Impact
DPDP Act, 2023	Data Privacy & Protection	High
RBI Cybersecurity Framework, 2023	BFSI Security Resilience	Very High
Telecom Security Mandate, 2024	Network Security Enforcement	High

Strategic Insights

- Government cybersecurity budget set to reach INR 20,000 crores (2025).
- Workforce growth: From 0.5 million (2022) to projected 2 million by 2030.



Cybersecurity Business Models

MSSP, Security-as-a-Service (SECaaS), and Incident Response

Key Business Models Overview (2025)

Model	Adoption (%)	Typical Annual Growth	Core Value Proposition
Managed Security Service Providers (MSSP)	70%	22%	24/7 Security monitoring, threat detection, & managed response
Security-as-a-Service (SECaaS)	85%	30%	On-demand, cloud-based security without upfront capital investment
Incident Response-as-a-Service (IRaaS)	65%	35%	Rapid breach containment and forensic capabilities

Strategic Insights & Key Metrics

- Global MSSP market expected to reach USD 70 billion by 2027, driven by escalating threats and skills shortages.
- SECaaS, growing faster at 30% CAGR, is forecasted to exceed USD 45 billion by 2027, fuelled by SMEs adopting flexible security models.

- Incident Response (IR) outsourcing adoption has increased by 50% since 2020, with average response times cut from 72 hours to less than 24 hours.

Top Challenges & Solutions in Business Models

- **Challenge:** High costs for in-house SOC operations
- **Solution:** Outsourced SOC via MSSPs (reducing costs by up to 40%).
- **Challenge:** Limited internal expertise
- **Solution:** IRaaS providers with guaranteed response SLA (75% reduction in resolution time).

Whoa! That's great to learn about this booming market.
But threats like ransomware and AI-attacks are surging even with a greater rate. Nations like India are responding with major new data protection laws, driving a swift evolution toward agile, as-a-Service security models. In all, the industry in India and on a global level is taking its shape towards a better tomorrow. But let's take a look that who is shaping this trend.. who knows, maybe we can lead this industry tomorrow?

Key Players and Leaders

Top Cybersecurity Platforms and Market Leaders (Global and India)

Market leadership in cybersecurity hinges on comprehensive, AI-driven platforms and agile, integrated solutions.

Global Cybersecurity Leaders (2025)

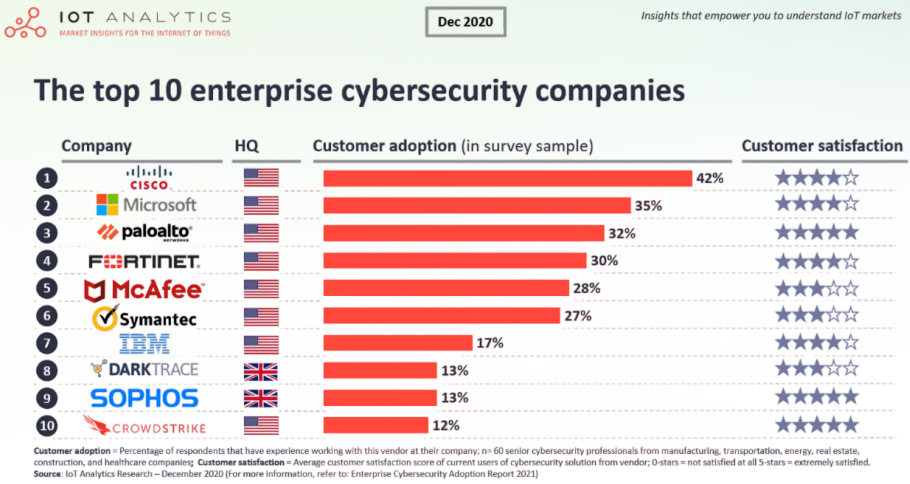
- Palo Alto Networks – Integrated XDR, zero-trust, and cloud security leadership.
- CrowdStrike – Endpoint security (EDR) market dominance, 60% YoY growth.
- Microsoft Security – Expanding Azure Sentinel ecosystem, market share at 25% globally.Regulatory Landscape Overview (2025)

Leading Indian Cybersecurity Companies

Company	Specialization	Major Clients	Revenue Growth
Quick Heal	Endpoint & Network Security	Govt, BFSI	20% CAGR
TAC Security	Vulnerability Management	Global Fortune 500	25% CAGR
Safe Security	AI Cyber Risk Quantification	BFSI, Global Insurance	30% CAGR

Investment Trends

- Cybersecurity startups attracted USD 1 billion annually (2025).
- M&A activities rising sharply with market consolidation.



This chart shows Cisco leading cybersecurity adoption at 42%, followed by Microsoft (35%) and Palo Alto (32%), with CrowdStrike and Sophos earning the highest customer satisfaction ratings.

Tech Influencers and Celebrity Voices in Cybersecurity

Top Tech Influencers in Cybersecurity

Kevin Mitnick

Kevin was once the world's most wanted hacker, but later became a celebrated white-hat hacker and cybersecurity consultant. He authored The Art of Invisibility, promoting personal privacy and awareness around digital tracking.

Katie Moussouris

She pioneered bug bounty programs at Microsoft and later founded Luta Security. She helped establish the responsible vulnerability disclosure standards now adopted worldwide by tech firms.

Edward Snowden

The former NSA contractor, became a global name after exposing U.S. government surveillance programs. His revelations triggered a worldwide debate on privacy rights, encryption, and digital sovereignty.

Kutcher

Apart from being a Hollywood actor, co-founded Thorn, a non-profit that tech to combat online child trafficking. He has addressed the U.S. Congress and global platforms on digital safety and cyber crime.

As the historians have quoted that – those who move forward with a vision, have a higher chance of winning over those with a plan. These great personalities and thought leaderships have defined the way this industry is getting shaped. The leading sets of companies have changed the consumer market and continue to do so in the longer run.

We believe, there is a long way to go and we've got a lot to learn.


Hey! Have you heard about the recent transitions and developments in cloud, network and other related domains? Let's move forward to find more interesting insights.


02

Insights and Thought Leadership

Latest Technology Trends

Global Trends and Growth Snapshot

EDR, Next-Gen AV, and Device Posture Management

Endpoint security is critical, protecting organizational endpoints amid rising remote work and sophisticated attacks, with endpoints accounting for over 80% of breaches.

Strategic Endpoint Security Technologies (2025)

Endpoint Security Type	Adoption	Breach Prevention Efficiency	Growth CAGR
Endpoint Detection and Response (EDR)	85%	90–95% reduction in successful endpoint breaches	28%
Next-Gen Antivirus (NGAV)	90%	80–90% malware detection	20%
Device Posture Management	70%	60–75% risk reduction	25%

Industry Best Practices

- Real-time EDR integration with SOC: Over 80% enterprises using EDR integrate directly into SIEM/SOAR solutions.
- Behavioral analysis in NGAV achieving 60% faster threat identification compared to traditional antivirus.
- AI-driven continuous posture assessments adopted by 65% of large enterprises, ensuring endpoint compliance in real-time

Key Endpoint Security Challenges & Mitigations

- Zero-day threats: Behavioral analytics used by 90% of NGAV providers.
- Endpoint visibility: Automated EDR tools deployed by 85% organizations, reducing mean-time-to-detect (MTTD) by 70%.

Network Security

Firewalls, IDS/IPS, SASE, and SD-WAN

Network security remains fundamental in an increasingly perimeter-less, hybrid work environment. Cloud-based SASE and SD-WAN adoption significantly transform security pos tures.

Key Network Security Technologies & Market Dynamics

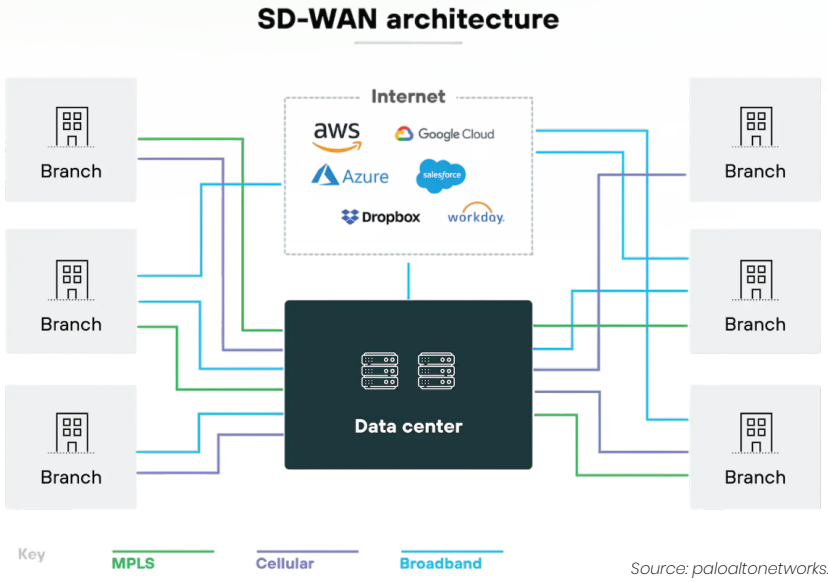
Technology	Adoption (%)	Annual Growth	Key Strengths
Next-Gen Firewalls	90%	15%	Deep packet inspection, integrated threat intelligence
IDS/IPS	80%	18%	Real-time intrusion detection, automated threat prevention
Secure Access Service Edge (SASE)	70%	35%	Integrated cloud-native security for remote workforce
Software-Defined WAN (SD-WAN)	75%	30%	Optimized connectivity, secure remote access

Strategic Network Security Trends

- SASE expected to exceed USD 20 billion by 2027 driven by hybrid workforce requirements.
- SD-WAN adoption cuts WAN management costs by 30–40%, with security enhancements through integrated firewall and VPN features.
- Unified threat management (UTM) devices now include IDS/IPS in 95% of deployments, ensuring robust perimeter security

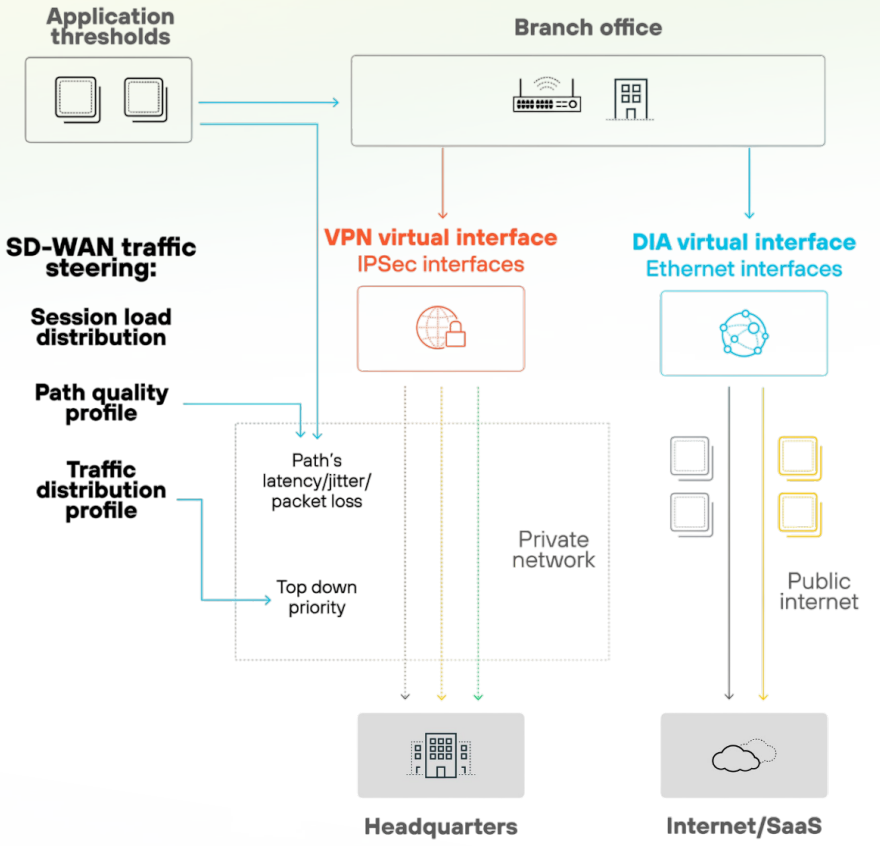
Strategic Recommendations for Enterprises

- Integrated SASE/SD-WAN solutions provide an average latency improvement of 25–30%, boosting employee productivity.
- Next-Gen Firewalls now standard in 90% of mid-to-large enterprises, providing enh nced threat visibility with real-time analytics.



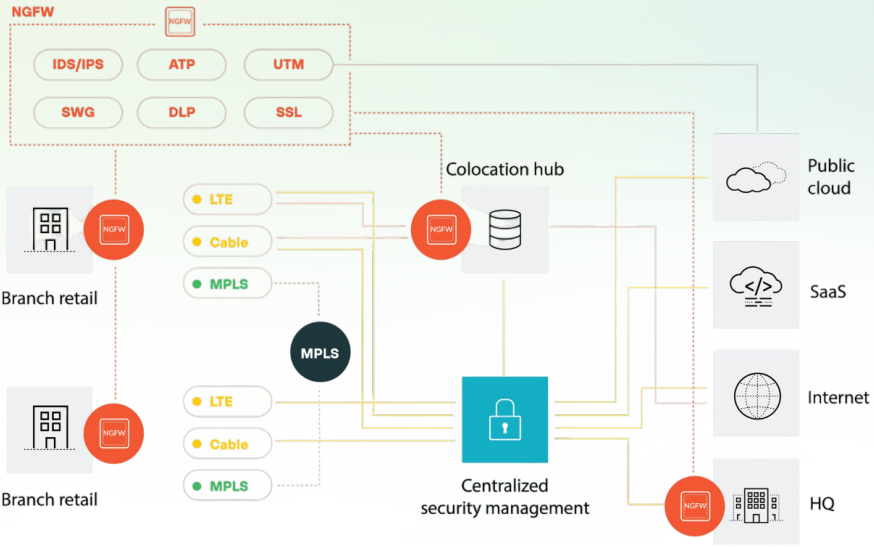
Source: paloaltonetworks.com

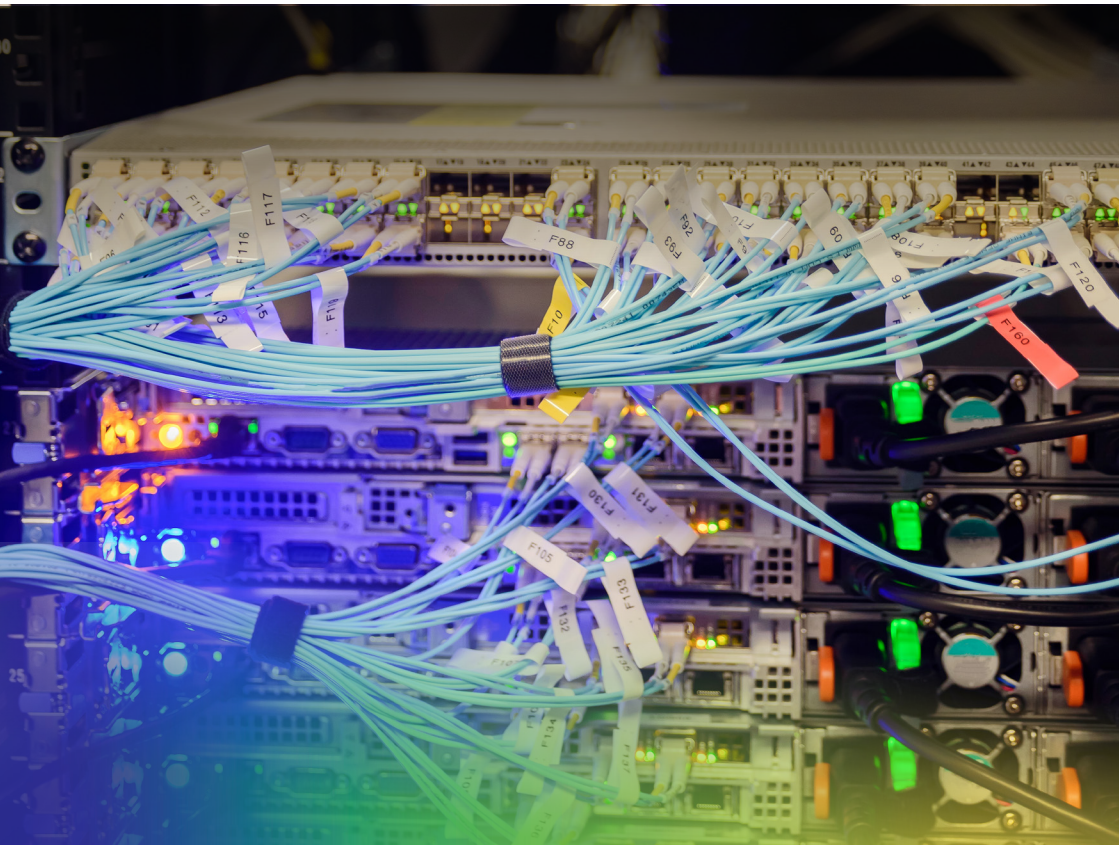
SD-WAN dynamic path selection and traffic steering



Source: paloaltonetworks.com

Secure SD-WAN deployment





Cloud Security

Cloud adoption accelerates cybersecurity complexity. Organizations rapidly adopt cloud-native security frameworks and automated platforms for better compliance and risk management.

Cloud Security Market Dynamics (2025)

Technology Category	Adoption (%)	Avg. Breach Reduction	CAGR
Cloud Security Posture Management (CSPM)	85%	75–85%	30%
Cloud-Native SIEM	70%	70–80% faster breach detection	25%
Container Security	75%	80–90% reduced container vulnerabilities	35%

Strategic Cloud Security Insights

- 85% enterprises adopt CSPM tools, significantly reducing misconfiguration-driven breaches.
- Cloud-native SIEM adoption accelerates incident response from days to hours for 75% of organizations.
- Container security investments growing rapidly at 35% CAGR, essential for securing DevOps environments.

Challenges & Strategic Approaches

- Cloud Misconfigurations: Automated CSPM tools detecting issues 80% faster, reducing breaches by 75%.
- Container Vulnerabilities: Integrated runtime protection adopted by 70% of enterprises, reducing attack surface by over 85%.
- Data Visibility: Cloud-native SIEM solutions ensuring unified visibility, adopted by 70% large enterprises.

Strategic Recommendations for Cloud Security

- Adopt integrated CSPM and container security solutions (60% cost savings in security operations).
- Real-time visibility via cloud-native SIEM helps meet compliance standards (up to 70% faster audit preparation).

Cybersecurity is the backbone of emerging technologies.

Application & API Security

WAF, DevSecOps, and Runtime Protection

Rapid digital transformation drives heightened application security requirements, particularly around APIs and cloud-native applications.

Application Security Best Practices (2025)

- Web Application Firewall (WAF): Blocks 90% of web threats; regulatory compliance standard.
- DevSecOps: Identifies and mitigates 60% of vulnerabilities pre-deployment.
- Runtime Application Self-Protection (RASP): Real-time defense, reduces exploits by 80%

Application Security Adoption Rates

Practice	Vulnerability Reduction	Adoption Rate
WAF	90%	85%
DevSecOps	60%	75%
RASP	80%	65%

Data Security & Privacy

Data has become the new currency, magnifying the necessity of stringent security and privacy measures to ensure compliance and business continuity.

Global Data Breach Landscape (2025)

- Annual global data breaches cost enterprises USD 12 trillion (up from USD 8 trillion in 2023).
- 60% of breaches involve compromised customer data. Runtime Application Self-Protection (RASP): Real-time defense, reduces exploits by 80%

Key Data Security Technologies & Impact

Technology	Technology	Key Verticals	Impact Metrics
Advanced Encryption Standards	85%	BFSI, Government, Healthcare	80% reduction in breach severity
Data Loss Prevention (DLP)	80%	Telecom, IT, BFSI	70% fewer internal data leaks
Tokenization	75%	Retail, Payments	65% reduction in PCI DSS breaches
Privacy Enhancing Technologies	70%	Healthcare, Government	90% compliance with GDPR/DPDP

Strategic Initiatives & Investments

- Data protection spending: Set to exceed USD 150 billion by 2027.
- Rapid shift towards zero-trust data architectures, witnessing a CAGR of 30%.

Ransomware

Evolution, Prevention, and Recovery Strategies

Ransomware remains a prime cybersecurity threat, accounting for over 45% of cyber insurance claims in 2025.

Ransomware Growth & Statistics (2025)

- Average ransom payments rose 400% since 2021, averaging USD 5 million per incident.
- Estimated global damages: USD 30 billion annually.

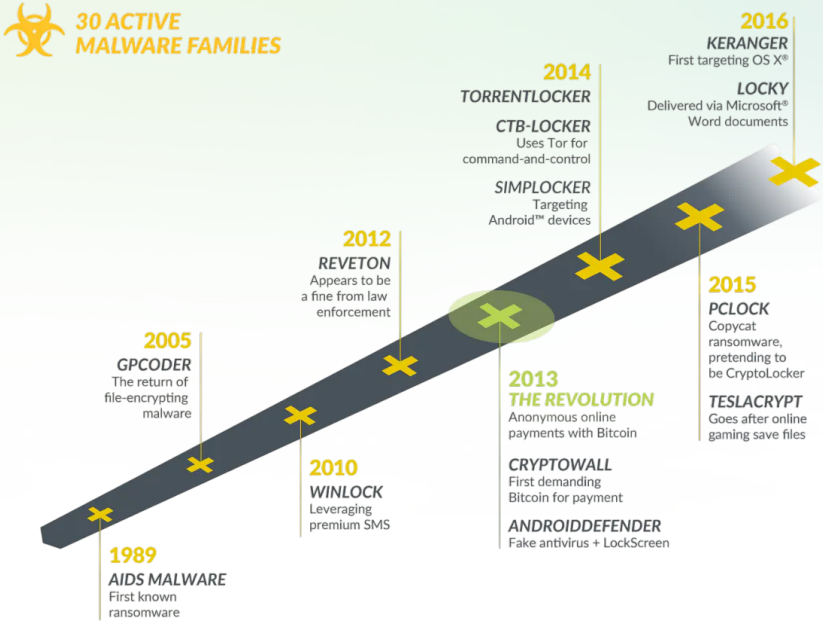
Notable Ransomware Groups & Major Attacks

Ransomware Group	Origin	Target Sectors	Prominent Incident (2024–25)
LockBit 4.0	Russia	Healthcare, Govt.	NHS (UK): Breach impacting 3M records
Conti	Russia	BFSI, Manufacturing	Toyota (Japan): 24-hour outage
DarkSide	Eastern EU	Energy, Critical Infra.	Petrobras (Brazil): $20M ransom

Prevention & Recovery Measures

- AI-driven detection tools reducing detection time by 70%.
- Immutable storage backups adoption (90%) halving recovery time.
- Cyber hygiene training reducing susceptibility to ransomware by 60%.

THE RISE OF RANSOMWARE



Source: paloaltonetworks.com

This timeline shows the rise of ransomware from the first AIDS malware in 1989 to modern families like Locky and Keranger, marking its evolution into a major global cyber threat.

Advanced Persistent Threats

APTs remain high-risk threats, targeting strategic industries and government infrastructure with growing sophistication.

APT Threat Landscape & Trends (2025)

- State-sponsored APTs represent 80% of critical infrastructure attacks.
- Average dwell time of APT actors within systems reduced from 150 days (2020) to 60 days (2025) due to advanced detection tools.

Notable APT Incidents (2024–25)

Incident	Actor	Sector	Impact & Damage
EU Energy Grid Disruption	Cozy Bear	Energy	NHS (UK): Breach impacting 3M records
Taiwan Semiconductor Breach	APT41	Semiconductor	IP theft worth USD 2B
Cryptocurrency Exchange Heists	Lazarus	BFSI	Combined USD 600M thefts

Strategic Countermeasures & Best Practices

- Adoption of MITRE ATT&CK frameworks in security operations by 70% of enterprises.
- Collaborative threat intelligence sharing platforms (CERT-In, NATO CCDCOE).

Upgrading the cybersecurity network is indispensible with growing industrial landscape.

Watchlist 2030

AI Security Orchestration, Autonomous Security Bots & Future Cyber Threats

By 2030, cybersecurity is fundamentally autonomous, orchestrated by highly advanced, self-governing AI-driven platforms and adaptive security bots. This paradigm shift will redefine human roles, focusing on strategic oversight rather than reactive incident management, transforming enterprise security posture into a proactive, predictive defense mechanism.

Strategic Forecast & Predictions (2030)

Autonomous Cybersecurity Bots Dominance:

- Autonomous cybersecurity bots are projected to handle an overwhelming 80% of all threat detection and response tasks, drastically reducing human intervention and accelerating resolution times from hours to mere seconds. These bots will leverage machine learning to adapt to novel threats in real-time, providing an unprecedented level of defense automation.

Explosive Growth in Global AI Security Orchestration Market:

- The global AI security orchestration market is forecast to surge, surpassing USD 60 billion by 2030, exhibiting a robust Compound Annual Growth Rate (CAGR) of 35% from its 2025 valuation. This growth is fueled by increasing enterprise demand for integrated, AI-powered solutions that centralize security operations and automate complex workflows.

Predictive Threat Intelligence Systems:

- By 2030, predictive AI models will enable organizations to anticipate emerging threats with 90% accuracy, allowing for pre-emptive defense strategies rather than post-breach reactions.

Zero-Trust Evolution to Trust-Less Ecosystems:

- The Zero-Trust model will evolve into a "Trust-Less" ecosystem, where every interaction, device, and user continuously undergoes rigorous AI-driven authentication and authorization, eliminating implicit trust boundaries entirely.

Emerging Future Cyber Threats & Solutions (2030)

Threat Category	Impact Level	Key Characteristics	Emerging Defense Technologies & Strategies	Adoption Rate (2030)
Quantum-based Breaches	Critical	Breaking classical crypto instantly.	PQC & QKD implementation.	75%
AI-generated Deepfakes & Social Engineering 2.0	High	Sophisticated phishing/ espionage.	Real-time detection, biometrics.	80%
Swarm-based Cyber Attacks	Critical	Millions of bots overwhelming defenses.	Autonomous counter-swarm defense.	65%
Bio-cyber Convergence Threats	-High	Exploiting biological system vulnerabilities.	Secure bio-sensor networks.	40%
Supply Chain AI Poisoning	High	Malicious data injection into models.	XAI validation, immutable registries.	70%

Strategic Imperatives for Cybersecurity Readiness by 2030

Ubiquitous AI/ML Integration:

- AI and Machine Learning will be non-negotiable foundations for all cybersecurity operations. Human oversight will pivot from reactive incident management to strategic governance, threat hunting, and the refinement of autonomous security systems.

Mandatory Autonomous Security Infrastructure:

- Autonomous security infrastructure will become a mandatory compliance and operational requirement for all enterprises globally, driven by regulatory bodies and the sheer volume and sophistication of threats.

Talent Transformation:

- The cybersecurity workforce will undergo a radical transformation, with a focus on AI ethics, quantum cryptography, and advanced threat intelligence analysis, shifting away from repetitive, manual tasks.

Global Cyber Resilience Alliances:

- Enhanced international collaboration and real-time threat intelligence sharing will be critical, formalizing alliances to counter nation-state and highly organized cybercriminal syndicates.

Having analyzed the industry-specific drivers, such as the modern digital battleground, detailing essential technologies like EDR and SASE that secure our endpoints, networks, and clouds. which spotlights the escalating threats like ransomware and nation-state APTs, before looking ahead to 2030, where autonomous AI bots and quantum-safe defenses will redefine our entire security future. it's time to assess how individual technologies are adapting to these pressures in our next section.


In a tech-heavy world, cybersecurity is a business imperative.

Interactions with Other Tech

IoT & OT Security

The explosive growth of IoT/OT deployments drives a parallel increase in vulnerability and complexity in security management.

IoT/OT Security Stats & Risks (2025)

- 50 billion IoT devices globally, rising to 100 billion by 2030.
- OT-related security incidents up 200% since 2020.

IoT/OT Security Solutions & Adoption

Solution	Adoption (2025)	Industries Impacted	Key Benefits
ICS/SCADA Endpoint Protection	80%	Manufacturing, Energy	75% breach prevention improvement
Taiwan Semiconductor Breach	75%	Smart Cities, Healthcare	70% faster vulnerability patching
Cryptocurrency Exchange Heists	70%	Automotive, Consumer IoT	Combined USD 600M thefts

Investment & Strategic Outlook

- Global OT security market to reach USD 50B by 2027.
- Zero-trust architectures adopted by 70% of IoT-enabled enterprises.

AI-Powered Attacks & Deepfake Threats

Detection and Defense

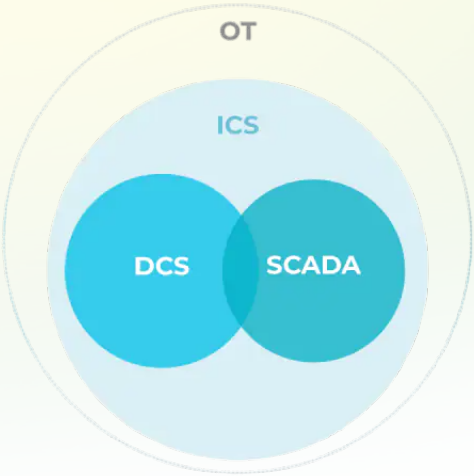
AI technology is weaponized in unprecedented ways, enhancing phishing effectiveness and proliferating deepfake threats.

AI-Powered Attack Landscape

- Deepfake fraud losses projected at USD 10 billion by 2026.
- AI-generated phishing effectiveness 3x higher than traditional methods.

Defensive Solutions & Effectiveness

Technology	Adoption	Defense Effectiveness
Deepfake Detection Algorithms	70%	85%
AI-based Email Filtering	75%	80%
Real-time Content Verification	65%	80%



OT, ICS, SCADA and DCS Systems

OT vs. ICS vs. SCADA Security

OT Security

- Covers a wide range of systems.
- Protects people, process, & profit.
- Defends against online threats.
- Manages physical devices & processes.

ICS Security

- Focus on industrial machiner control.
- Ensures data integrity & machinery safety.
- Links to physical safety.
- Utilizes preventitive & responsive defenses.

SCADA Security

- Centers on real-time data & control.
- Involves risk & compliance management
- Essential for national security.
- Focuses on public safety & services continuity.

Source: paloaltonetworks.com

Quantum Computing

Quantum Threats and Quantum-Resistant Cryptography

Quantum computing brings revolutionary security threats, necessitating a rapid move towards quantum-resistant cryptographic standards.

Quantum Threat Scenario (2025)

- Quantum capabilities estimated to break standard RSA encryption within 1 day by 2026.
- Early quantum breaches predicted in BFSI and Defense sectors by 2028.

Quantum-Resistant Solutions

Technology	Adoption 2025	Industry Priority	Impact
Quantum-Safe Algorithms	60%	Government, BFSI	Protect sensitive national data
Quantum Key Distribution	50%	Telecom, Defense	Highly secure communications

Cybersecurity Workforce

The escalating cybersecurity skills gap demands strategic workforce investment. Global shortage projected to reach 3.5 million professionals by 2027.

Key Workforce Metrics (2025)

- Cybersecurity professional demand outpacing supply by 70% globally.
- Average cybersecurity salaries up 40% from 2020, driven by severe talent shortage. Quantum-Resistant Solutions

Critical Cybersecurity Roles & Salaries (Global Avg.)

Role	Avg. Salary (USD)	Required Certifications
CISO	250,000–400,000	CISSP, CISM, MBA
Cybersecurity Analyst	100,000–160,000	CISSP, CEH, CompTIA CySA+
Penetration Tester	120,000–180,000	OSCP, CEH, GPEN
Security Engineer	110,000–175,000	CISSP, GSEC, AWS/GCP cert.

Strategic Initiatives to Bridge Skill Gap

- Public-private cybersecurity education partnerships (India, USA, EU) aiming to train over 2 million professionals by 2028.
- Industry-recognized certifications mandated in 90% of hiring by large enterprises.

Now that we've explored the emergence and adaptation with other technologies such as Quantum security, workforce and IoT, let us seek that how we can make the most of this opportunity within the industry set guidelines

Ecosystem Leadership

Global Regulatory Environment

GDPR, CCPA, HIPAA, DPDP Act & Cybersecurity Policy Frameworks

Rapid digital transformation is driving tighter global cybersecurity regulations. Non-compliance now carries unprecedented financial and reputational risks. Key Workforce Metrics (2025)

Major Global Cybersecurity Regulations (2025)

Regulation	Region	Sector Impacted	Key Compliance Areas	Penalties
GDPR 2.0	EU	Cross-sector	Enhanced data portability, real-time audits	EUR 50M or 6% global revenue
CCPA/CPRA	USA	Tech, Retail, BFSI	Consumer rights enforcement, breach disclosure	USD 20M per violation
HIPAA	USA	Healthcare	Patient data encryption, detailed audit logs	USD 5M per incident
DPDP Act 2023	India	Cross-sector	Data localization, explicit consent management	Up to INR 500 crore per breach
China CSL 2.0	China	Tech, Financial services	Data sovereignty, localization, periodic audits	Up to USD 10M fines and business suspension

Strategic Global Compliance Trends

- Global compliance spending projected to exceed USD 60 billion by 2026.
- Adoption of automated compliance monitoring tools reaching 85% in large enterprises.
- Average spend on compliance audits per company growing 30% annually due to complexity.

Audit, Compliance & Risk Management

Audit, risk management, and incident response capabilities form the cornerstone of modern cybersecurity governance.

Strategic Metrics & Benchmarks (2025)

Capability	Enterprise Adoption	Impact & Results
Annual cybersecurity audits	95%	80% fewer regulatory violations
Real-time incident response	85%	Incident resolution accelerated by 60%
Continuous risk assessments	75%	Reduced average breach cost by 50%

Incident Response Framework Best Practices

- MITRE ATT&CK Framework usage at 80% adoption, boosting attack pattern recognition.
- Crisis simulation drills conducted quarterly by 70% of Fortune 500 companies.
- Cyber resilience plans mandatory in 85% of publicly traded firms globally.

Global Investments & Growth

- Cyber risk management software spending to reach USD 40 billion by 2027.
- Incident response automation tools CAGR projected at 28% from 2025-2030

Source: hyperproof.io/

Cybersecurity Insurance

Risk Transfer, Underwriting, and Incident Response Coverage

Cyber insurance has transitioned from niche risk coverage to essential business protection amid escalating cyber threats.

Cyber Insurance Global Market Overview (2025)

- Total Market: USD 30 billion, CAGR 22% from 2020.
- Average premium increases at 25% annually due to higher claim rates.
- Top sectors insured: BFSI (85%), Healthcare (70%), IT/Tech (65%), Manufacturing (60%).

Coverage and Premium Metrics

Sector	Avg. Annual Premium (2025)	Common Coverage	Avg. Claim (2025)
BFSI	USD 2–5M	Data breach, ransomware	USD 10–15M
Healthcare	USD 1–3M	Privacy breach, HIPAA fines	USD 5–8M
Manufacturing	USD 1–2M	OT disruption, ransomware	USD 5–10M

Strategic Underwriting Trends

- Real-time security posture assessment integration by insurers adopted by 70% of leading firms.
- Cyber Risk Quantification (CRQ) platforms deployed in underwriting at 60% of insurers.

Driving business from niche risk coverage to essential business protection

Awareness and Simulation-Based Training

Human factors remain the leading cybersecurity vulnerability, accounting for 95% of successful breaches.

Global Phishing Threat Landscape (2025)

- Phishing attacks increasing annually by 40%.
- Average financial loss per phishing incident: USD 2.8 million.

Phishing Resilience Metrics (2025)

Training Type	Adoption	Reduction in Phishing Success
Interactive Simulation	85%	60%
Regular Awareness Tests	80%	55%
AI-Based Training	60%	75%

Cyber ranges and simulation-based platforms are critical for realistic, hands-on cybersecurity training.

Global Cyber Range Market & Growth (2025)

- Global cyber range market valuation: USD 12 billion, CAGR of 35%.
- Over 90% of national cybersecurity agencies implementing cyber range exercises.

Cyber Range Adoption and Benefits

Sector	Adoption Rate	Key Benefits
Government	90%	Improved critical infra. Protection
BFSI	85%	Better incident response capabilities
Defense	95%	Real-time warfare simulation

Global Investment in Awareness Training

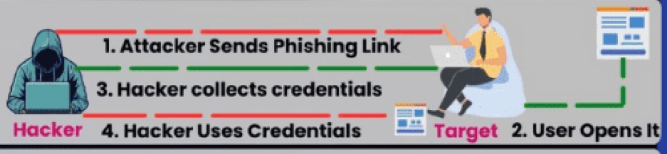
- Global cybersecurity training market projected to reach USD 15 billion by 2027 (30% CAGR).
- Advanced gamified cybersecurity training adopted by 70% of Fortune 500 companies.
- Integration of AI-driven attack simulation used by 60% of cyber ranges.
- International cyber warfare simulation drills conducted annually by NATO, APAC alliances.

Top 8 Cyber Attacks

Ethical Hackers Academy

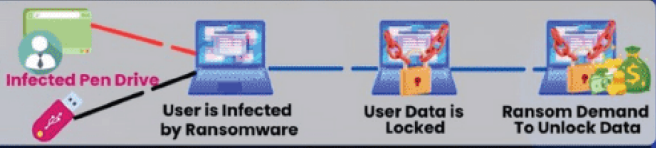
1 Phishing Attack

The use of deceptive emails, texts, or websites to gain sensitive information.



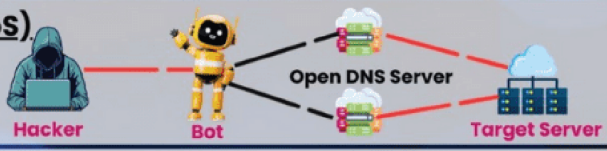
2 Ransomware

Malware that can encrypt data and make you pay to get them back.



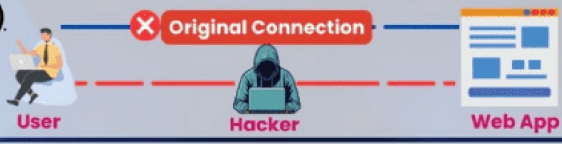
3 Denial-of-Service (DoS)

Loading excessive load on a machine or network so that it stops working normally.



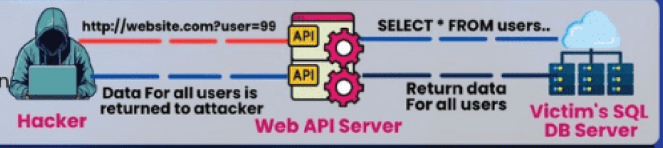
4 Man-in-the-Middle (MitM)

Engaging in covert interception and manipulation of communication between two parties without noticing it.



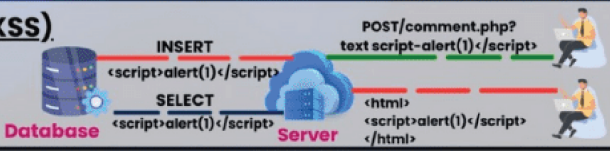
5 SQL Injection

To get the Access to the database, Vulnerabilities in Database queries can be exploited



6 Cross-Site Scripting (XSS)

Putting malicious code into websites that other people visit.

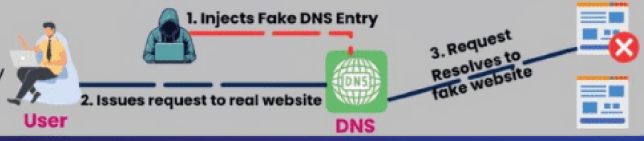


7 Zero-Day Exploits

Attacks take advantage of unknown vulnerabilities before programmers can fix them.

8 DNS Spoofing

Sending DNS queries to malicious sites so that they can be accessed without permission.



Source: zeronetworks.com

This infographic shows eight major cyberattack types—including phishing, ransomware, DoS, MitM, SQL injection, XSS, zero-day exploits, and DNS spoofing—that exploit vulnerabilities to steal data or disrupt systems.

These systems do set us a mile ahead of our competition, isn't it mate?

Setting us with a base where we are able to collaborate with the system in an ethical and planned manner. Now let us understand that what the industry experts have to say about our future with this technology and how do they perceive this opportunity from a different angle.

03

IMC 2024 Discussions and Engagements

Panelists

Mr. Satinder Pal Singh
Former Director (Security), Ministry of Home Affairs; Secretary, North Eastern Council

Mr. Jong Bum Park
President & CEO, Samsung India

Panel Title

The Expanding Role of Telecom Service Providers in Ensuring Cybersecurity

Mr. Akshay Aggarwal

Senior Cybersecurity & Risk Leader, KPMG India

Moderator

Panelists

Mr. Siddharth Talawadekar
VP & Business Head – IoT, Bharti Airtel Digita

Mr. P. K. Gupta
Senior Executive, C-DOT (Cybersecurity & Network Analytics Solutions)

Mr. Lt. Gen. (Retd.) S. P. Kochhar
Director General, COAI

Top Highlights of the talk

Mr. Akshay Aggarwal, Senior Cybersecurity & Risk Leader, KPMG India – Moderator

Mr. Aggarwal asserted that telecom networks are now "critical infrastructure for everything else," requiring operators to evolve into integrated security partners. He framed the discussion around expanding 5G/IoT threat surfaces, telco responsibilities, and how regulation must make security a built-in capability.

Mr. Satinder Pal Singh, Former Director (Security), MHA; Secretary, North Eastern Council

Mr. Singh asserted that national security agencies rely heavily on telecom networks, making telco cybersecurity a matter of national resilience. He stressed the need for secure-by-design networks, robust lawful intercept frameworks, and deep coordination to counter sophisticated cross-border threats.

Mr. Jong Bum Park, President & CEO, Samsung India

Mr. Park asserted that device and handset security is integral as endpoints are often the weakest link. He highlighted Samsung Knox as hardware-rooted security, arguing that robust ecosystem security—from chip to network—is essential to maintain trust in a hyper-connected 5G world.

Mr. Siddharth Talawadekar, VP & Business Head – IoT, Bharti Airtel Digital

Mr. Talawadekar asserted that the rapid proliferation of IoT devices drastically enlarges the attack surface, invalidating perimeter-only models. He explained Airtel's focus on secure IoT connectivity, SIM/eSIM-based identity, and network-level anomaly detection baked into design.

Mr. P. K. Gupta, Senior Executive, CDOT (Cybersecurity & Network Analytics)

Mr. Gupta asserted that indigenous security solutions like C-DOT's platforms are crucial for India to gain visibility into threats across its backbone. He underlined that AI-based anomaly detection and deep packet inspection enable early detection and reduce reliance on foreign black-box systems.

Mr. Lt. Gen. (Retd.) S. P. Kochhar, Director General, COAI

Mr. Kochhar asserted that operators face dual pressure to invest heavily in cybersecurity while keeping services affordable. He called for updated regulatory frameworks and incentives to encourage telcos to invest in quantum-safe crypto and Zero-Trust architectures for 5G-Advanced and 6G.

Conclusion

The consensus is that telcos must fundamentally shift to integrated security partners, driven by national security needs and the expanded 5G/IoT attack surface. Success requires aligning regulatory incentives with commercial viability, implementing secure-by-design architectures (from chip to network), and fostering indigenous threat intelligence. their compliance burden without compromising user rights, arguing that a constant process of fine-tuning the regulation is necessary as technology evolves.

IMC 2025 Discussions and Engagements

Panelists

Mr. Vinay, CEO
Data Security Council of India (DSCI)

Miss Shweta Singh
General Manager, Policy and Strategy, Airtel

Panel Title

Privacy and Protection at the Edge – Operationalising India's Data Protection Act

Sush Yash Kalash

Senior Manager, Digital Ecosystem, GSMA

Moderator

Panelists

Mr. Vinit Malik
Director, Telecommunication Engineering Center (TEC), Government of India

Mr. Kapil Chadri
Partner, Denton Link Legal

Dr. Jaijit Bhachara
President, Center for Digital Economy Policy Research (C-DEP)

Top Highlights of the talk

Mr. Vinayak Godse

Mr. Vinay urged pivoting security from governance to architectural solutions, stressing that privacy and innovation are not a "zero-sum game." He championed Privacy Enhancing Technologies (PETs) like homomorphic encryption and questioned how AI's "intelligence" layer will redefine concepts like Fiduciary and Processor under the Act.

Miss Shweta Singh

Miss Singh praised the "Data Fiduciary" term and the avoidance of "consent fatigue" by allowing existing customer notification. She cited major hurdles: unclear processor liability (especially for overseas clients) and the urgent need for harmonization across sectoral regulators to simplify compliance.

Mr. Vineet Malik

Mr. Malik framed the government's role as facilitating business while ensuring data sovereignty. He highlighted initiatives like BIVS and the Digital Consent Management pilot to achieve a 'One Nation One KYC' vision, emphasizing the need for regulatory coherence to prevent excessive fiduciary obligations.

Mr. Jaijit Bhachara

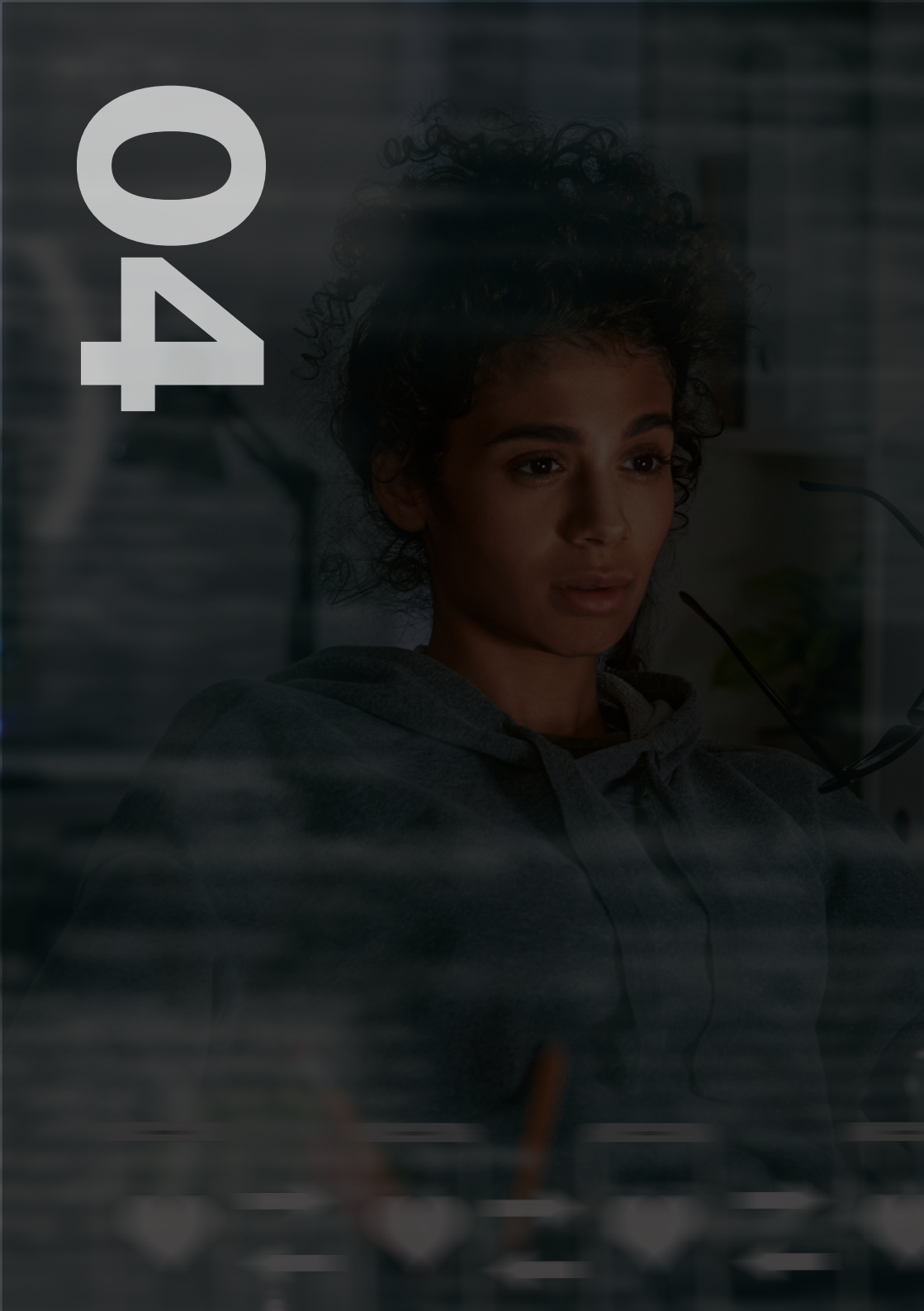
He focused on ambiguity at technology's "edges," specifically children's consent (shared devices) and consent for the incapacitated. He called for carving out provisions for startups to ease their compliance burden, advocating for constant regulatory fine-tuning.

Mr. Kapil Chadri

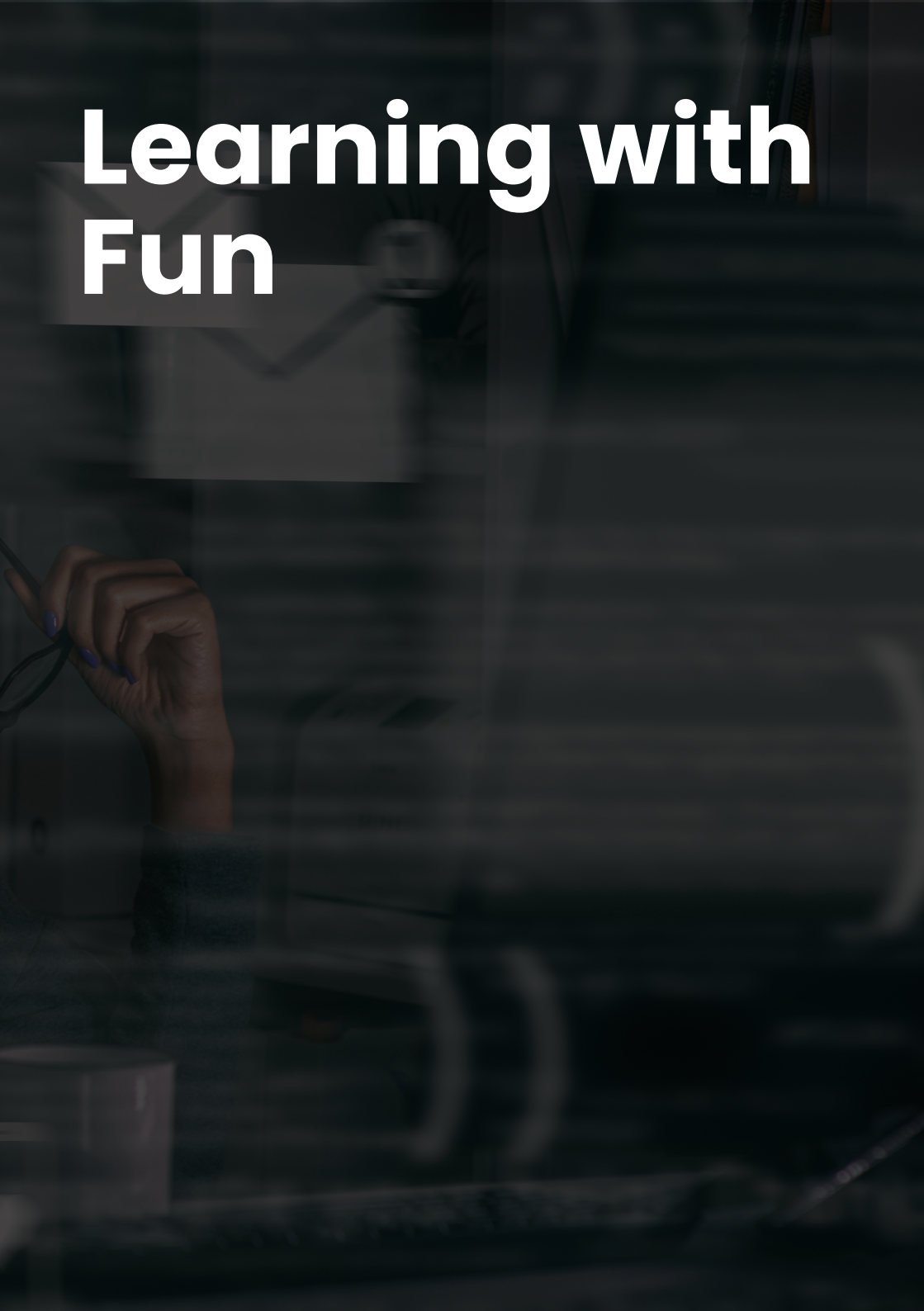
Mr. Chadri provided practical legal counsel, prioritizing data inventory and establishing a DPO. He targeted two barriers: the mandate for fresh consent every three years (limiting long-term user journeys) and the "biggest elephant in the room"—frictionless parental verification for children's consent.

Conclusion of the Conference

The consensus was that the successful operationalization of the DPDP Act rests on finding the median ground between balance and purpose. The moderator summarized the collective wisdom: success requires Clarity in Governance, Privacy by Design, Consistency in User Experience, and Inclusion, all built on a foundation of Trust through Transparency. The core implementation challenge is moving beyond regulatory checklists (the "what") and embracing architectural innovation and cross-sectoral synergy (the "how") to ensure India's digital economy is both innovation-first and privacy-protected.


04

Learning with Fun



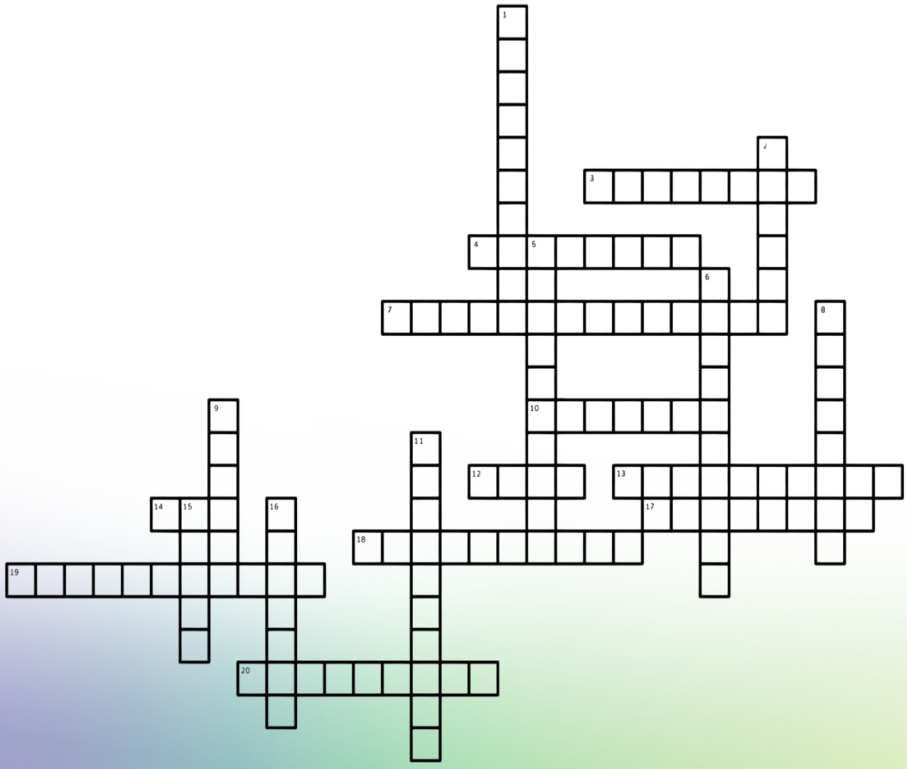
Crossword & Puzzle

Across

3. Combination for account access
4. Network security barrier
7. Process of confirming identity
10. Computer virus, spyware, etc
12. Unsolicited email or messages
13. Data scrambling for protection
14. Virtual private network for secure online browsing
17. Scam email targeting personal information
18. Unauthorized access to sensitive information
19. Malicious activity on a computer system
20. Software to protect against viruses and malware

Down

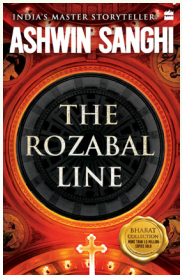
1. Criminal activity in cyberspace
2. Malicious software disguised as legitimate
5. Malware that demands payment for data return
6. Unique physical characteristics used for identification
8. Device connected to a network
9. Collection of hacked computers controlled remotely
11. Trial-and-error method to obtain passwords
15. Update to fix security vulnerabilities
16. Unauthorized access to a computer system



Find the Words

P N M A L W A R E E O P T Y A F E N
D A H I D E N T I T Y T H E F T O N
E T S O I E U H O N E Y P O T I G C
N C S S D P E K I A R S C Y T K N P
I R A B W N P E R A C Y T C L O I E
A Y N O A O N A S G E W E H I R T I
L P D O H E R A S T B T C T M I A L
O T B U A A R D D S E P A T O Y N E
F O O S C B A R C D W C M L U I T P
S J X S K N R F N R I O P E C H I P
E A I N I B T O L T A X R O D R V H
R C N C N B I E N T E C G D L P I I
V K G O G S E E R Y N Y K T F O R S
I I B G U S H E A C N P I I T X U H
C N S R C T K D A Y H F C O N P S I
E G T E U A O F I R E W A L L G M N
C N T A K R S E N C R Y P T I O N G
I O N Y E P L I S B D A M K E G U T
C A E Z B I O M E T R I C S W U N C
S B R U T E F O R C E A T T A C K O

Cybersecurity In Literature

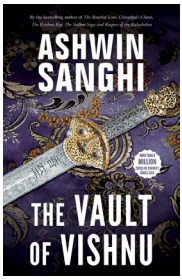


The Rozabal Line – Ashwin Sanghi

While primarily a religious thriller, the book subtly explores encrypted communications, identity spoofing, and surveillance, blending geopolitics with cyber tactics — a hallmark of modern disinformation warfare.

The Vault of Vishnu – Ashwin Sanghi

A modern techno-thriller that touches on cyber-espionage, AI weaponry, and hacking in the context of Sino-Indian conflict. It mirrors real-life hybrid warfare, mixing state secrets and digital intrusions.

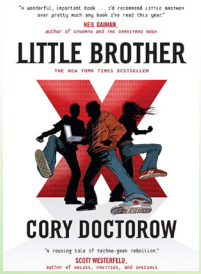


Neuromancer – William Gibson (1984)

The foundational cyberpunk novel that coined "cyberspace". It follows Case, a washed-up hacker navigating virtual landscapes, AI manipulation, and corporate cyber warfare. Gibson essentially predicted modern cybersecurity decades ahead.

Little Brother – Cory Doctorow (2008)

A young adult novel that doubles as a cybersecurity manifesto. When a teen is detained by Homeland Security after a terrorist attack, he starts an encrypted resistance using public-key cryptography and hacking, exposing surveillance overreach.



Sci-Fi Films

Enthiran (Robot) — 2010

In Shankar's visionary film, an AI robot named Chitti is reprogrammed with feelings, leading to chaos. The film highlights the threat of unauthorized access and AI manipulation, serving as a metaphor for advanced malware turning on its creator. The core theme is cyber-vulnerability of autonomous systems.

Irumbu Thirai — 2018

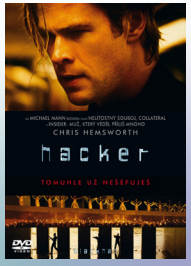
A gripping techno-thriller where the antagonist is a cyber-criminal who steals data for financial extortion. It portrays real-world threats like phishing, social engineering, and the dark web with surprising accuracy, making cybersecurity central to the narrative.

The Matrix — 1999

A landmark film where the entire human experience is simulated through code. It explores themes of digital control, surveillance, and hacking into simulated systems — a metaphor for breaking out of digital illusions and regaining agency over data-driven realities.

Blackhat — 2015

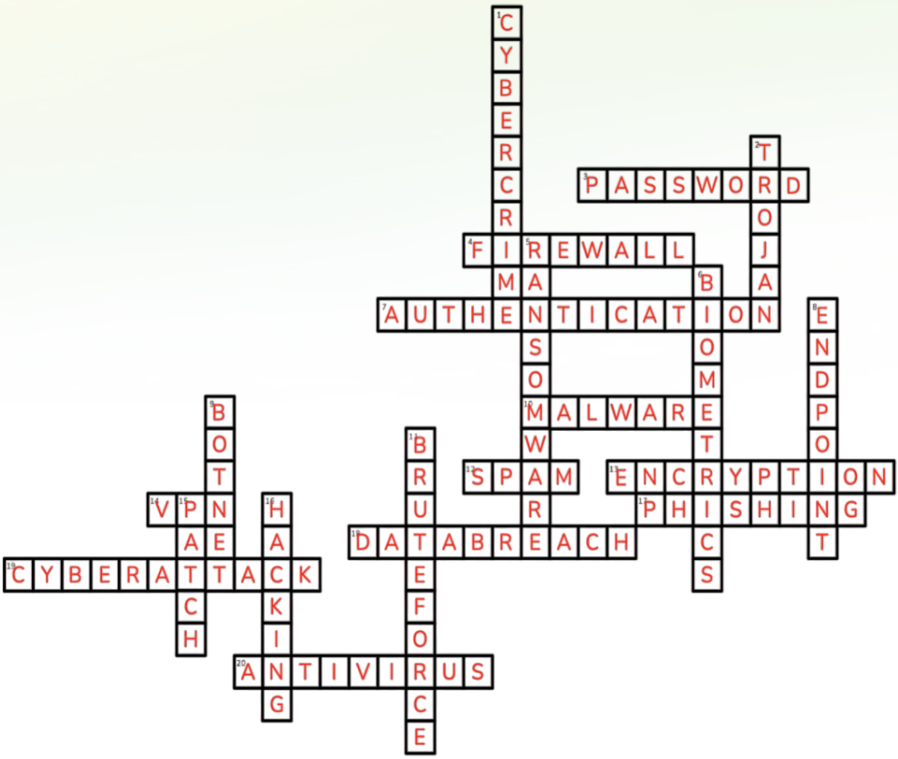
A thriller where a hacker is released from prison to stop a cybercriminal network. The film dives into state-sponsored cyberattacks, SCADA system breaches, and exploit-based warfare, showing the geopolitical dimension of cybersecurity.



Comic Strip


THE CURIOUS CASE of
CAPTAIN CLICKBAIT
CYBERSPACE INC., MONDAY
WOW! 'YOU'VE WON A FREE IPHONE! -THIS HAS TO BE REAL!
POOF! ENTER... CAPTAIN CLICKBAIT!
WE'VE GOT MEA AND AI MONITORING!
BUT ALL IS NOT LOST...
WOURS MINE
WE'VE GOT MFA AND AI MONITORING!
DRAMATIC FIGHT..
I'M IN YOU'RE SYSTEM!
NOT IF YOU'RE SANDBOXED FIRST,
THAT WAS CLOSE...
THINK "WRS CLOSE
REMEMBER, TEAM — THINK BEFORE TOU CLICK.
CYBERSECURITY IS EVERYONE'S JOB
NO MORE FALLING FOR CAPTAIN CLICKBAIT —

Antivirus
Cryptojacking
Hacking
Malware
Sandboxing
Authentication
Denial of Service
Honeypot
Password
Zero Day Exploit
biometrics
Encryption
Identity Theft
Password cracking
Bruteforce Attack
Firewall
Intrusion Detection
Phishing


CYBERCRIME
PASSWORD
FIREWALL
MALWARE
AUTHENTICATION
BOTNET
SPAM
ENCRYPTION
VPN
HACKING
BRUTEFORCE
DATABREACH
PHISHING
CYBERATTACK
ANTIVIRUS
ENDPOINT

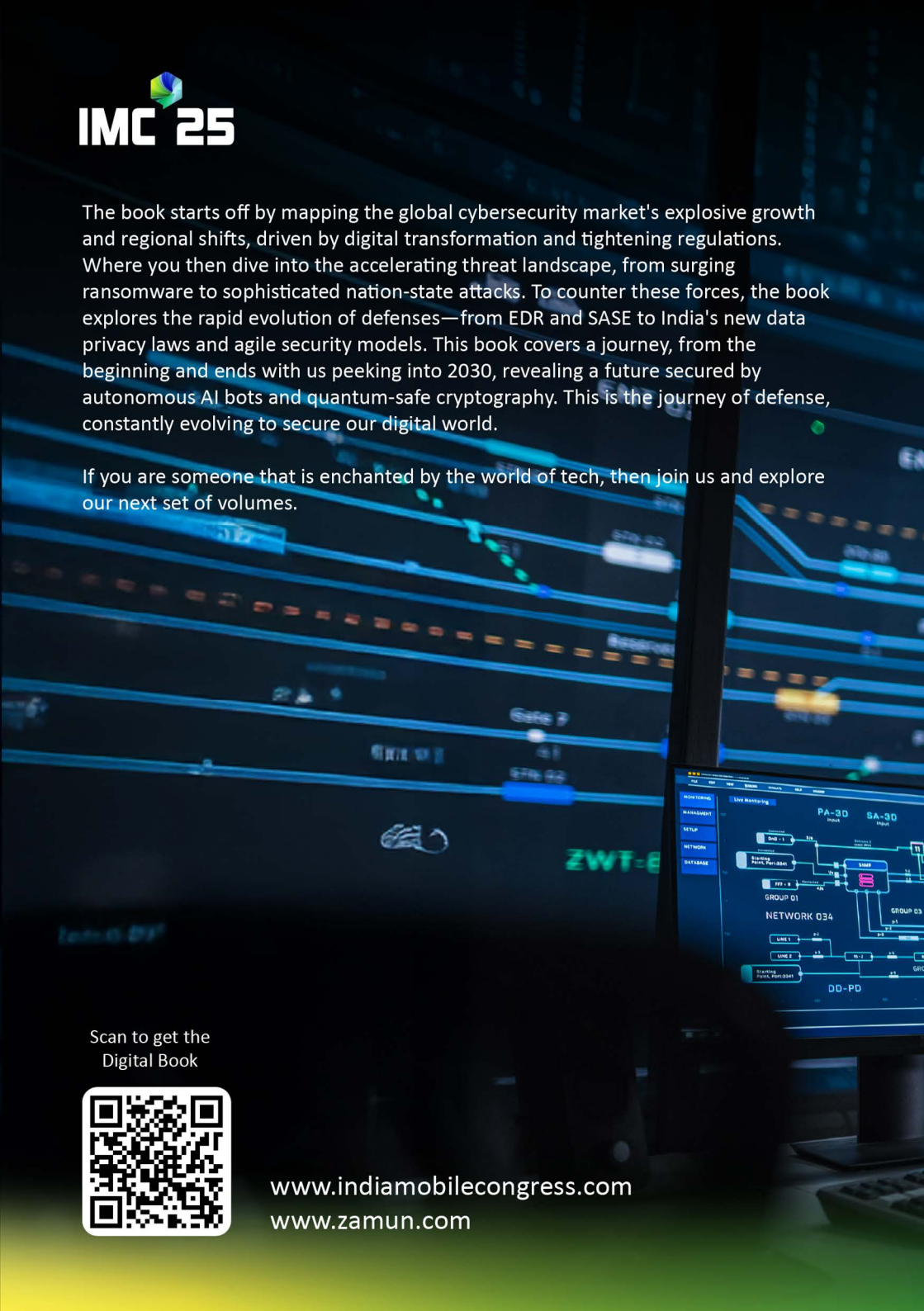
Bibliography

1. https://www.optiv.com/insights/discover/downloads/zero-trust-infographic
2. https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard
3. https://www.drishtiias.com/daily-news-analysis/national-cyber-security-strategy-1
4. https://iot-analytics.com/leading-enterprise-cybersecurity-companies-2021/
5. https://www.paloaltonetworks.com/cyberpedia/what-is-secure-sd-wan
6. https://unit42.paloaltonetworks.com/unit-42-ransomware-trends/
7. https://www.paloaltonetworks.com/cyberpedia/ot-vs-ics-vs-scada-security
8. https://hyperproof.io/resource/it-risk-assessment/
9. https://zeronetworks.com/blog/mitigating-top-cyber-threats-2025-zero-trust-segmentation

IMC 25

The book starts off by mapping the global cybersecurity market's explosive growth and regional shifts, driven by digital transformation and tightening regulations. Where you then dive into the accelerating threat landscape, from surging ransomware to sophisticated nation-state attacks. To counter these forces, the book explores the rapid evolution of defenses—from EDR and SASE to India's new data privacy laws and agile security models. This book covers a journey, from the beginning and ends with us peeking into 2030, revealing a future secured by autonomous AI bots and quantum-safe cryptography. This is the journey of defense, constantly evolving to secure our digital world.

If you are someone that is enchanted by the world of tech, then join us and explore our next set of volumes.



Scan to get the Digital Book

www.indiamobilecongress.com
www.zamun.com