Meet The Presenter

Chand Raina (CK)

Head of Sales & Relationships

State Government Business - India

Tata Consultancy Services (TCS)

Chand.raina@tcs.com

+91 9987006393

Linkedin - linkedin.com/in/chaandkraina

About

- 22+ years of Industry Experience
- Designed, Built & Operated some of the world's largest shared services (RNPO, Essar, OTON)

Educational Qualifications & Certifications

- Bachelor of Engineering – NIT Surathkal
- MBA. Finance – IBS
- Certified 'Disruptive Innovation" and "Growth & Transformation" leader from Harvard Business School and INSEAD respectively
- Certified Blockchain and IoT Consultant

Publications (Key)

- The CPO balanced scorecard (How to leverage enterprise synergies in sourcing and procurement) – SCMR USA
- Reimagining the procurement operating model for tomorrow – SCMR USA
- Digitalizing Shared Services - ITSupplyChain
- Strategic View on Creating Synergies in Large Multi-Business Conglomerates (special focus on mergers and acquisitions situations) – tcs.com
- Blockchain – A Myth or A Reality (Tata McGraw Hill Print)

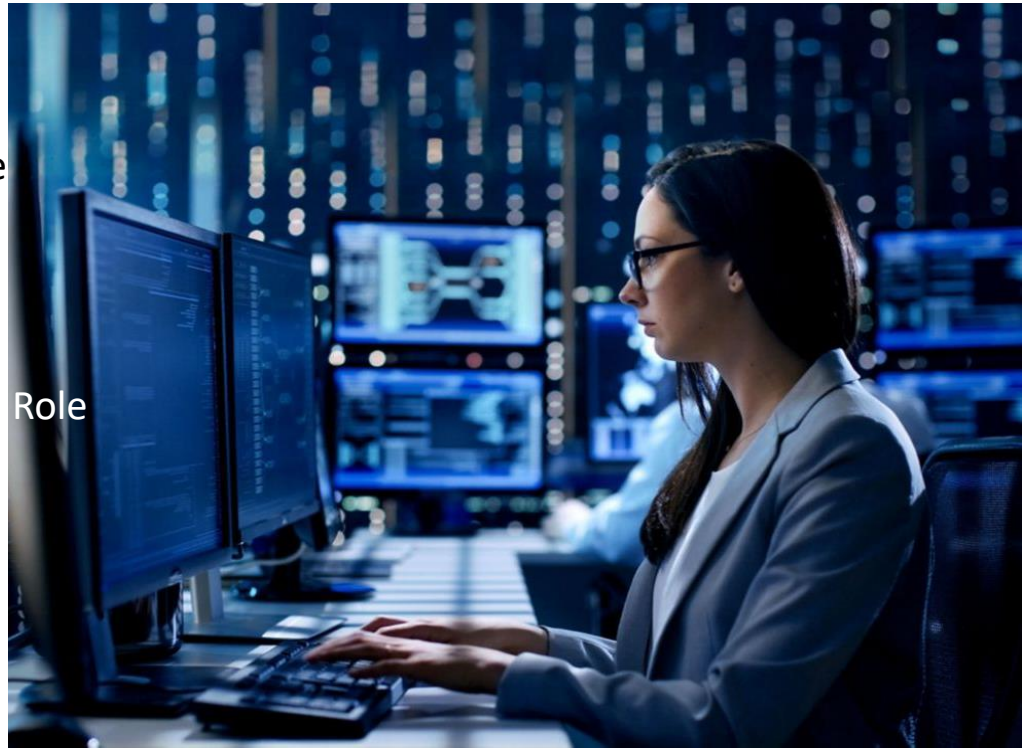
And, wrote this as well

TATA CONSULTANCY SERVICES

TATA

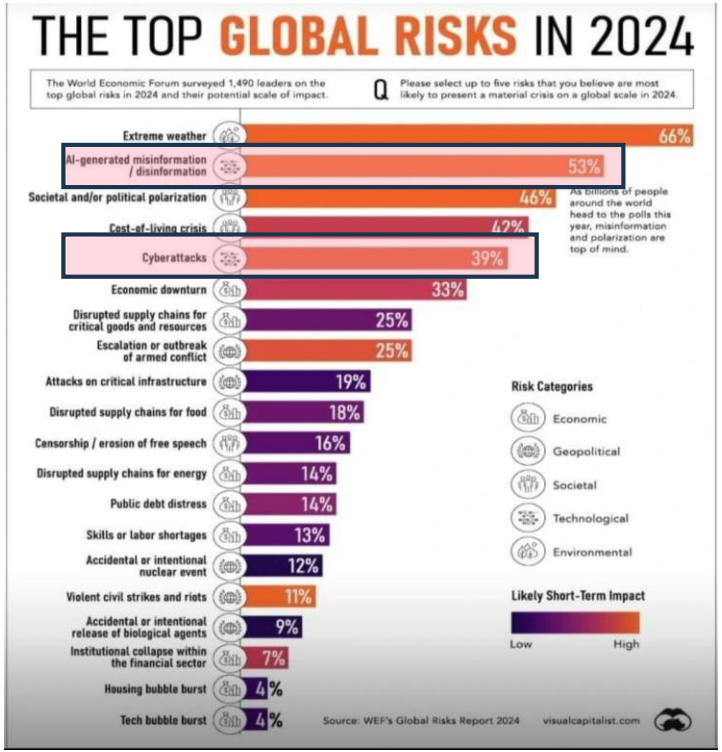

TATA CONSULTANCY SERVICES
TATA
Cybersecurity and
Emergency Response Readiness

1. Staying Ahead – Trends Shaping The Future
2. Incident Prevention & Response Readiness
3. Guardians of Digital Realm – Big Brother's Role
4. Prevention – Staying Ahead



Staying Ahead – Trends Shaping The Future

Identify | Protect | Detect | Respond | Recover



* World Economic Forum (WEF) - Source

* Crippling ransomware attack or a breach of sensitive consumer data

CYBERSECURITY TRENDS IN 2024

- ✓ **Ransomware Surge** – Sophisticated attacks on businesses and critical infrastructure
- ✓ **Zero Trust Security** – Assume distrust, enforce strict access control
- ✓ **Remote Work Security** – Secure endpoints, remote access methods

- ✓ **AI & ML in Cybersecurity** – Utilize for threat detection, anomaly
- ✓ **Cloud Security Challenges** – Secure Cloud Infra, misconfigurations
- ✓ **IOT & OT Security** – Vulnerable Internet of Things, Operational Tech

- ✓ **Cybersecurity Regulations** – Compliance enforcement to safeguard businesses data and critical infrastructure
- ✓ **Identity & Access Management (IAM)** – JML, MFA
- ✓ **Supply Chain Vulnerabilities** – 3rd Party vendors and Suppliers for access

- ✓ **Incident Response & Threat Hunting** – Proactive & reactive, planning
- ✓ **Privacy & Data Protection** – Compliance with Regulations, GDPR, CCPA
- ✓ **AI-Powered Cyber Threats** – Use of AI by Cybercriminals for sophisticated and targeted attacks, continuously evolving threats to Cybersecurity

Ransomware payments tracked exceeded $1.1 billion in 2023
Ransomware revenue had dropped to $567 million in 2022.
Source: SCM*

TATA CONSULTANCY SERVICES

TATA

Cyber Security In Summary

High Exposure

- Cam4 Data Breach (Mar 2020) – 10 billion data records exposed.
- Aadhaar Data Breach (Mar 2018) – ~ 1 billion citizens of India.
- It doesn't need a strong SME to pose a cyber threat.

At Stake

- $445 Bn impact on global economy annually
- The reputation and future damage makes it worse
- Compromising 'National Security' could have dire consequences

Know-what

- 63% data breaches come from exploiting internal weak points
- Foresight and strategic approach
- Proactiveness and resilience

Master the journey

- Know – what
- Leverage advanced technologies
- Maintain ethical and responsible practices

* https://en.wikipedia.org/wiki/Data_breaches_in_India#:~:text=India's%20Aadhar%20data%20breach%20was,private%20information%20like%20biometric%20data.

What Do You See Here!!

Voldemort: The Unseen Cyber Threat That Disguises, Morphs & Escapes

The **Many Faces** of Voldemort - Evolving Cyber Threats -Voldemort, the dark wizard, is known for his ability to disguise himself and his followers

The **Polyjuice Potion** Voldemort's followers use Polyjuice Potion to take on different identities. Cyber attackers could build any fake, social engineering etc to get entry into the network.

Voldemort's Horcruxes, fragments of his soul hidden in various objects, ensure his survival even when defeated. It is like malware which spreads thin & is impossible to eradicate completely

The Chamber of Secrets was concealed within Hogwarts, holding dangers that were difficult to detect. Every enterprise / govt department must be aware about this chamber

The **Dark Mark** signals the presence of Death Eaters. A chilling warning that bigger attack is on its way and the system is compromised.

Harry Potter's journey involves understanding **Voldemort's tactics** **and finding ways to counter them**

TATA CONSULTANCY SERVICES

TATA

It Is An Ongoing Fight Till Tough Voldemort Is Contained

Dumbledore's mentorship provides Harry with the knowledge and tools needed to confront Voldemort

The Order of the Phoenix - **Collaborative Defense-** The Order of the Phoenix unites to fight against the dark forces

The Patronus Charm - Proactive Defense Measures - Harry's mastery of the Patronus Charm is a **proactive defense** against Dementors

The Final Battle - **Incident Response and Recovery** - In the final battle at Hogwarts, Harry and his allies prepare and respond decisively to Voldemort's attack

Conclusion - **Vigilance and Adaptability** - Just as Harry remains vigilant and adaptable in his fight against Voldemort, our approach to cybersecurity and emergency response must be dynamic

Guardians of Digital Realm – Big Brother's Role

Technology

Advance Threat Detection System

Innovation

GenAI, AI/ML, Blockchain

Ecosystem mindset

Collaborative – Public Private Partnership

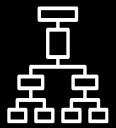
Awarness

Legal & Regulatory Framework, Education

Organizational agility

Cybersecurity Emergency Response Team

Structure



Modular & Centre-led

Governance

Global Engagement & Diplomacy

Prevention

- Create an inventory of assets, including hardware, software, and data
- Audit your network for unknown computers and services
- Disable internet-facing systems, services, and ports you don't need (3389, SMB 445, 135, 139, 22, 21)
- Perform regular vulnerability scans & Patch systems regularly, prioritize. Decommission EOL systems
- Ensure systems are properly hardened with security features enabled
- Secure remote access with MFA, password policy & lockouts
- Deploy endpoint security software (EDR, XDR) on all endpoints and servers
- Cybersecurity awareness training & awareness
- Implement Usecases, process for reporting and responding to suspicious activity (SOC Usecases)

- Email security across the entire enterprise
- Network segmentation to subdivide your networks
- Use least-privilege access for all systems and users including Service Accounts
- Restrict the use of legitimate tools commonly used by attackers (Psexec, PingEasy, PS etc)
- Harden domain controllers
- Monitor your network and endpoints using EDR, IDS, AV, and SIEM/SOC
- Maintain continuous data backup and restore process and make sure at least one backup is offline. Rehearse the restoration process
- Create an incident response plan that aligns with regulations
- Create a critical asset list so you know what you need to restore first
- Whitelisting Applications to ensure authorized software run.

TATA CONSULTANCY SERVICES

TATA

Thank you