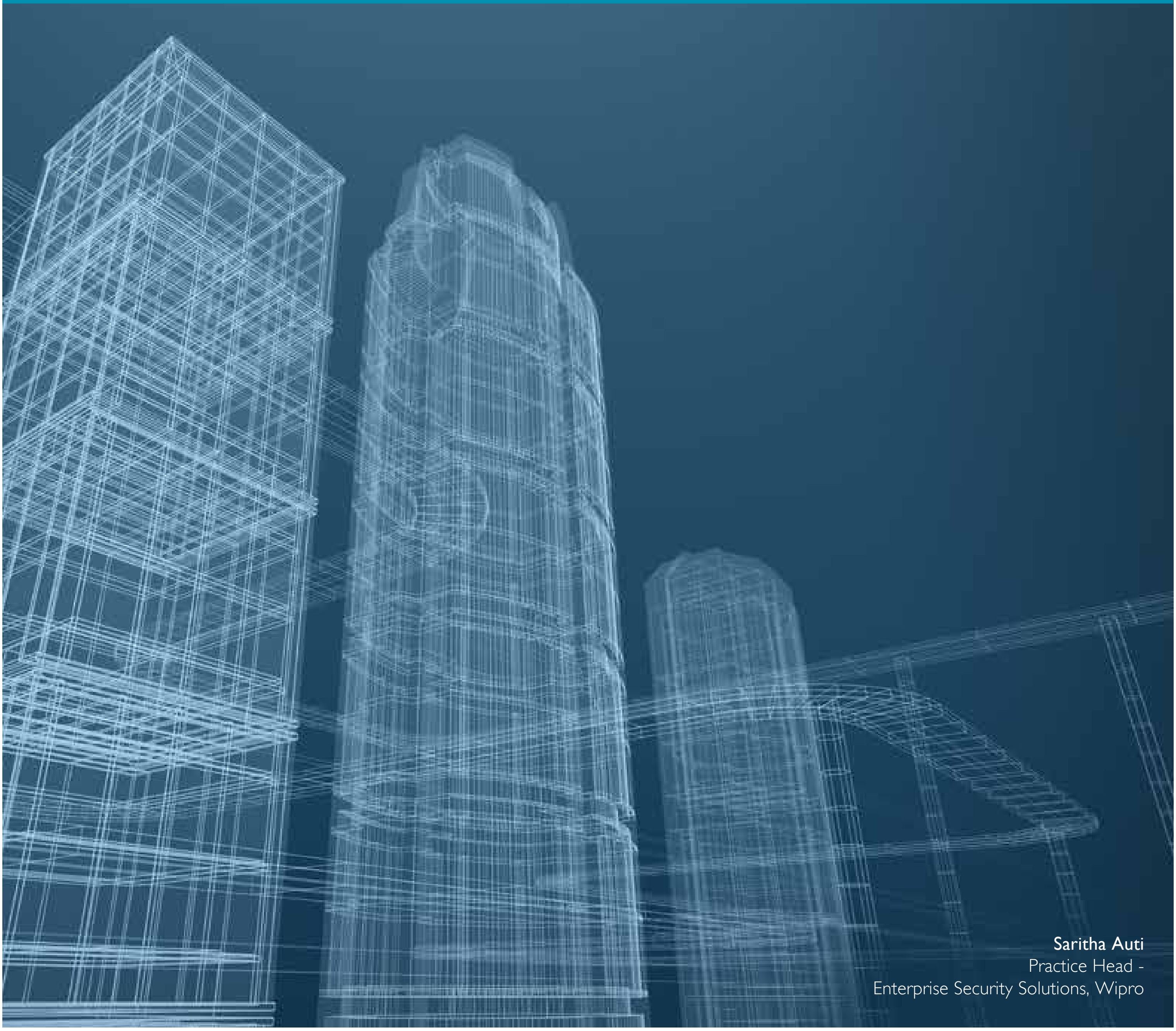
RESILIENCE AGAINST CYBER ATTACKS

Protecting Critical Infrastructure Information



Saritha Auti
Practice Head -
Enterprise Security Solutions, Wipro

Table of Contents

Abstract

The recent increase in the frequency and impact of cyber-attacks have kept Critical Infrastructure companies on their toes, fearing the worst for their organizations if an attack occurs on their critical infrastructure. A recent news article published by the New York Times states that cyber attacks are on the rise against corporations in the United States, with a particular focus on Energy companies. Reports of an attack similar to the Shamoon – Saudi Aramco attack are expected but the impact of such an attack in the United States would be of a magnitude much greater than Shamoon. These threats have made governments across the world wake up and take notice of Critical Infrastructure Protection as one of their highest priorities.

Why is Infrastructure Critical?

An infrastructure becomes critical when a disruption to this infrastructure results in irreversible and enormous loss (e.g. loss of life, environment etc.). The growing threat of international terrorism led policy makers to reconsider the definition of "infrastructure" in the context of specific non-functional requirements (NFR) of the business. These NFRs included Security, Performance, Availability, Integrity and Confidentiality (SPAIC). Each business has its own definition of SPAIC based on the regulatory requirements and country specific policies.

Critical Infrastructure is always associated with regulatory requirements and key resources who are directly handling the critical infrastructure. As such, any intentional or unintentional disruption to these will have a significant impact on the environment and life.

The following areas are considered to be a part of Critical Infrastructure:

- Agriculture
- Food
- Utilities - Drinking water and sewage management system
- Government
- Defense
- Oil and Gas infrastructure
- Nuclear Power Plants and the facilities that produce, use, store, and dispose off nuclear material
- Energy - production, transmission, and distribution services and critical facilities
- Special events of national significance
- Healthcare - drug discovery and development, patient information
- Banking and Finance
- Process industries
- Transportation - including railways, highways, shipping ports and airports & civilian aircrafts
- Livestock, agriculture, and systems for the provision of water
- Communication links
- Public and privately owned information systems with critical business data (e.g., information about oil reserves, information within Stock Exchanges, information about nuclear programs, drug research data, privacy information, financial data etc.)

There is an impending need for countries to develop a national critical infrastructure strategy which will provide a comprehensive and collaborative approach to enhance the resiliency of critical infrastructure. This common approach will enable partners to respond collectively to risks and target resources to the most vulnerable areas of critical infrastructure.

Guidelines to Defining a Successful Critical Infrastructure Protection (CIP) Strategy

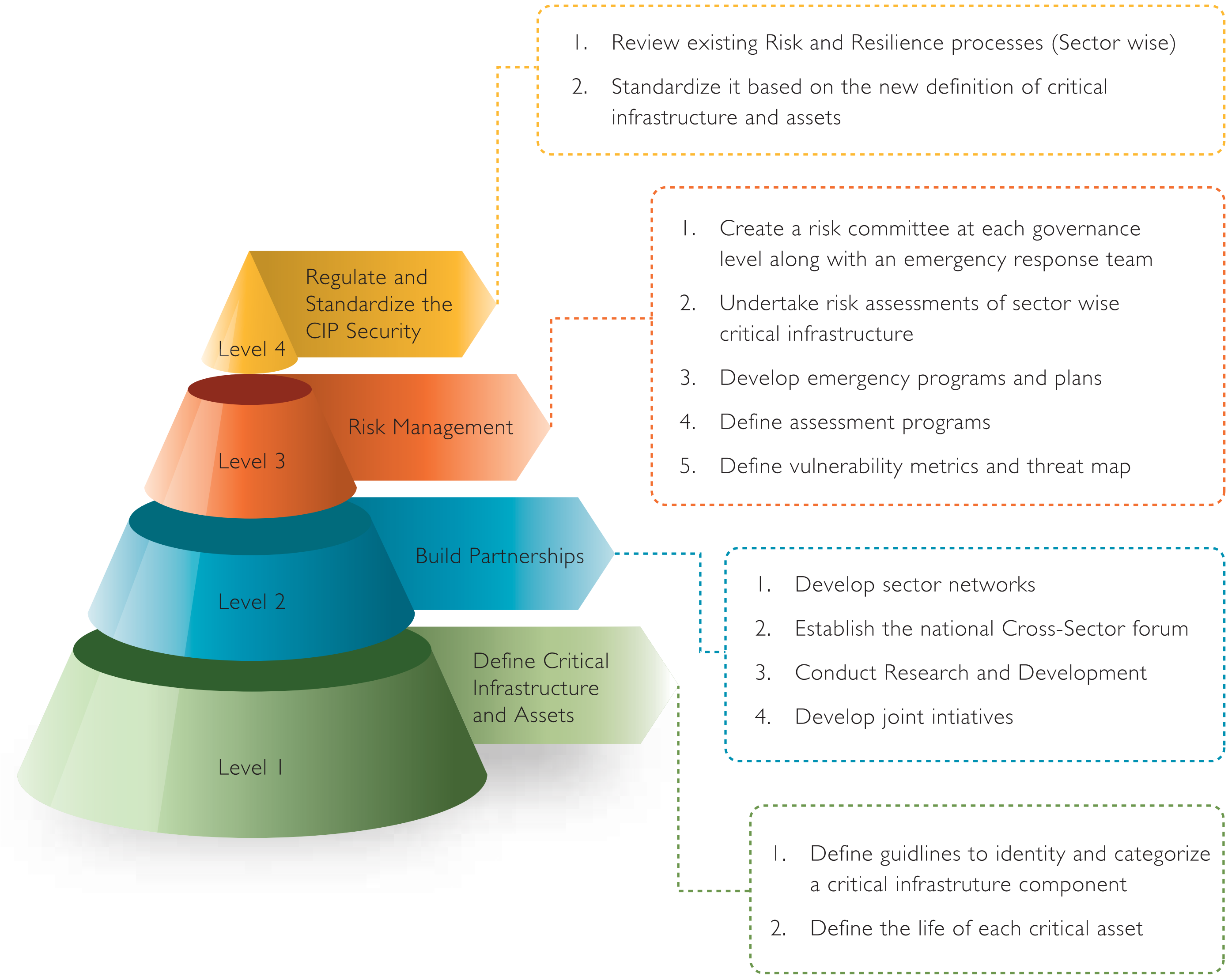
Industry leaders suggest that the government and the private sector should collaborate to protect a nation's critical infrastructure. This collaboration calls for the development of trusted partnerships to build regulatory requirements, governance processes, and resilience options jointly based on the existing mandates and responsibilities. The strategy should outline mechanisms to:

1. Create a government owned CIP Forum to share information about potential threats and disruptions through a highly confidential government owned body. Discussions in this forum should:
    a. Feed into the regulatory enhancements as a continuous improvement program
    b. Create awareness in both urban and rural areas
2. Create guidelines to protect critical assets and information
3. Build country specific risk frameworks for each critical infrastructure with guidelines to define asset criticality
4. Build a RACI (responsibility, accountability, consulted, informed) matrix

The Strategy should:

1. Put the onus on Critical Infrastructure companies to give high priority to the protection of their critical infrastructure
2. Should be defined considering Central Governments, States, Districts, and City Corporations responsible for protecting their own critical infrastructure and for supporting owners and operators in addressing this challenge
3. Enhance the resiliency of critical infrastructure through an appropriate combination of security measures to address human induced intentional threats, business continuity practices to deal with disruptions and ensure the continuation of essential services, and emergency planning to ensure adequate response procedures are in place to deal with unforeseen disruptions to critical infrastructure

Actionizing the Strategy for a Safer Future


Regulate and Standardize the CIP Security
Level 4
Risk Management
Level 3
Build Partnerships
Level 2
Define Critical Infrastructure and Assets
Level 1

1. Review existing Risk and Resilience processes (Sector wise)
2. Standardize it based on the new definition of critical infrastructure and assets

1. Create a risk committee at each governance level along with an emergency response team
2. Undertake risk assessments of sector wise critical infrastructure
3. Develop emergency programs and plans
4. Define assessment programs
5. Define vulnerability metrics and threat map

1. Develop sector networks
2. Establish the national Cross-Sector forum
3. Conduct Research and Development
4. Develop joint intiatives

1. Define guidlines to identity and categorize a critical infrastruture component
2. Define the life of each critical asset

Cyber Security and Critical Infrastructure

Cyber security for critical infrastructure depends a lot on the sector to which the critical infrastructure belongs.

Its objectives are:

1. Integrated security operations platform – This should provide a single platform where logs are collected, correlated, analyzed. This platform should collect logs from both IP and non IP devices, should be intelligent to dynamically build rules to eliminate False Positives
2. Unified Security view – The platform should be built on regulatory requirements, country specific rules, risk framework, criticality of assets and information. It should be based on Security Analytics framework which will score incidents, identify patterns and provide security and risk posture of the critical infrastructure at any point of time. An extension to this is predictive analysis which should help predict threat patterns and help sectors to plan mitigation
3. Resilience strategy – It is the quickness with which the critical infrastructure can bounce back after disruption. This should primarily be the Disaster Recovery and Business Continuity Plan for Critical Infrastructure. This is more of a policy and process which should be reviewed at pre-defined schedules for readiness

Broadly, cyber security can be classified into the following components for all Sectors:

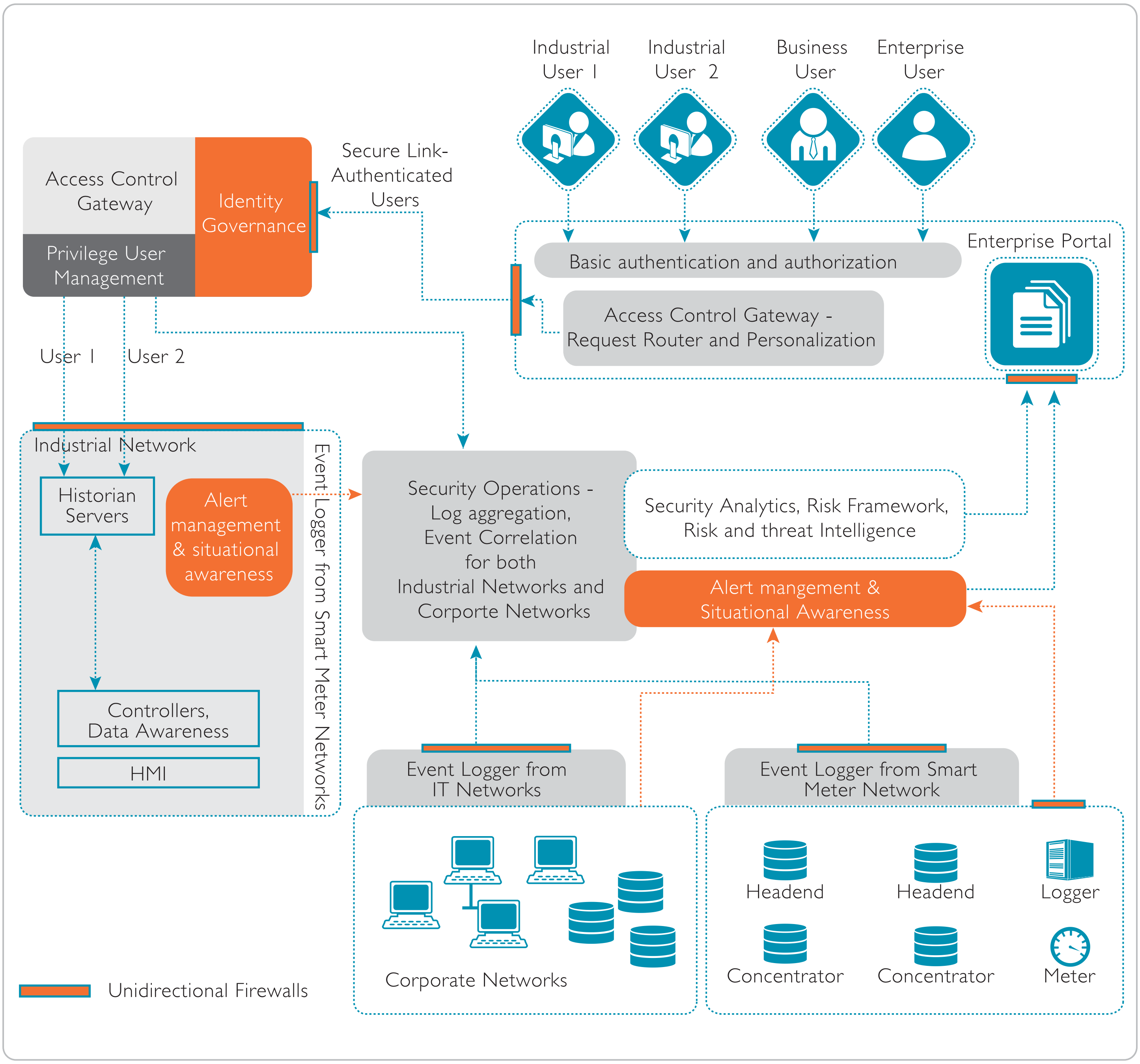
1. Cyber Security Governance
2. Security Convergence Platform
3. Integrated security operations
4. Security Analytics
5. Risk and Threat Intelligence

Illustration: Example of Industrial Control Systems Networks

Cyber security is becoming important for critical infrastructure due to the latest technology implementations like IP communications, BYOD policies etc. Similar to IT Infrastructure, Critical Infrastructure has its share of vulnerabilities that can't be addressed due to the proprietary nature of the OS and hardware. These devices are not regularly patched as the hardware patch release cycle is adhoc or longer than software patches.

This being the problem statement, the critical infrastructure component becomes vulnerable to malwares, advanced persistent threats and service disruption. In general, ICS networks lack features like monitoring, metrics, analytics and intelligence to predict threats. The solution should be capable of handling known problems and zero day vulnerabilities.

Solution for securing Industrial Control Systems Networks

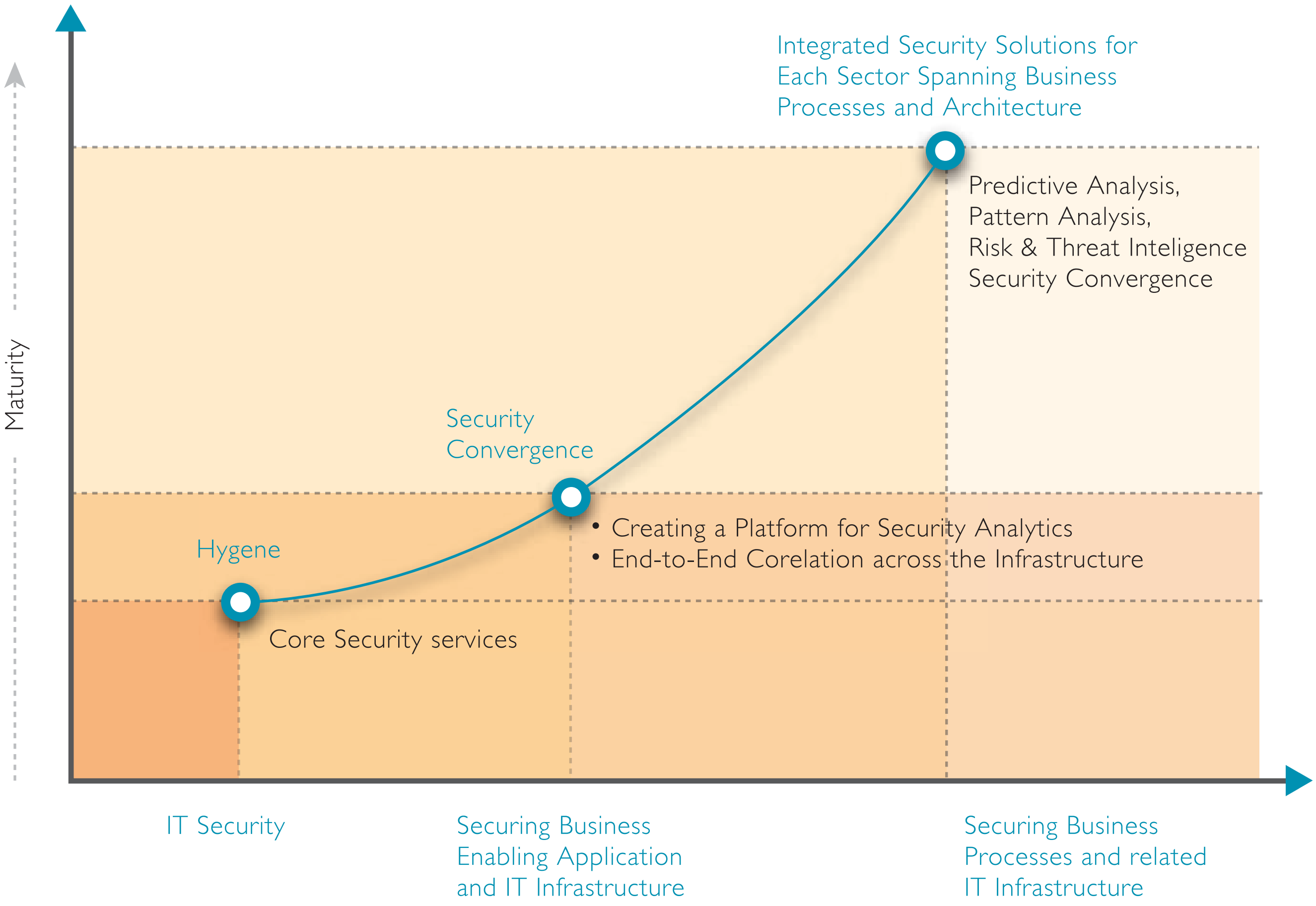


Industrial User 1
Industrial User 2
Business User
Enterprise User
Access Control Gateway
Identity Governance
Privilege User Management
Secure Link-Authenticated Users
Enterprise Portal
Basic authentication and authorization
Access Control Gateway - Request Router and Personalization
User 1
User 2
Industrial Network
Historian Servers
Alert management & situational awareness
Controllers, Data Awareness
HMI
Event Logger from Smart Meter Networks
Security Operations - Log aggregation, Event Correlation for both Industrial Networks and Corporte Networks
Security Analytics, Risk Framework, Risk and threat Intelligence
Alert mangement & Situational Awareness
Event Logger from IT Networks
Event Logger from Smart Meter Network
Corporate Networks
Headend
Headend
Logger
Concentrator
Concentrator
Meter
Unidirectional Firewalls

The solution platform should address the issues mapping the solution-to-sector specific value chain, applying global regulatory requirements and defining points of vulnerability to address known and unknown threat vectors.

Cyber Security Solution Roadmap

Cyber security for critical infrastructure should be broadly developed as per the roadmap shown in the illustration below


Maturity
Integrated Security Solutions for Each Sector Spanning Business Processes and Architecture
Predictive Analysis,
Pattern Analysis,
Risk & Threat Inteligence
Security Convergence
Security Convergence
• Creating a Platform for Security Analytics
• End-to-End Corelation across the Infrastructure
Hygene
Core Security services
IT Security
Securing Business Enabling Application and IT Infrastructure
Securing Business Processes and related IT Infrastructure

The level of maturity of a Cyber Security solution for CIP needs to progress through the stages shown in the illustration, gradually making the transformation from Core Security Services to Security Convergence and finally to Integrated Security Solutions – which involve predictive analytics and intelligence spanning business processes and architecture.

Conclusion

The implications of a Critical Infrastructure collapse are huge and need to be looked at from a long-term perspective. Close synergies between the government and the private sector need to be present to develop a comprehensive and robust strategy for thwarting off impending threats from politically motivated groups, cyber criminals and other such rogues. Steps should be taken to ensure CIP across all layers of CI Architecture, with components addressing business and operational processes, applications, data, communication, network and perimeter for IT and Operations Technology Network.

About the Author

Saritha Auti, Practice Head - Enterprise Security Solutions, Wipro

Saritha has over 17 years of experience in Enterprise Security & Architecture, spanning a wide gamut across product development, application security, systems integration, Enterprise Architecture and security architecture consulting. She heads Enterprise Security Architecture and Industrial Security Practice for Wipro with specific focus on Critical Infrastructure Security. She has devised several security solutions and architecture strategy for Oil & Gas, Telecom, Financial Sectors, Utilities, Defense, and has lead Security Architecture transformation programs. Apart from technology she is an ardent trekker, culture enthusiast and loves connecting with people.

To know more, contact: saritha.auti@wipro.com

About Wipro Ltd.

Wipro Ltd. (NYSE:WIT) is a leading Information Technology, Consulting and Outsourcing company that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology" - helping clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, a practitioner's approach to delivering innovation and an organization wide commitment to sustainability, Wipro has a workforce of 140,000 serving clients across 61 countries.

For more information, please visit www.wipro.com.

WIPRO
Applying Thought

DO BUSINESS BETTER

NYSE:WIT | OVER 140,000 EMPLOYEES | 61 COUNTRIES CONSULTING | SYSTEM INTEGRATION | OUTSOURCING

WIPRO TECHNOLOGIES, DODDAKANNELLI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA. TEL : +91 (80) 2844 0011, FAX : +91 (80) 2844 0256, Email: info@wipro.com
North America South America United Kingdom Germany France Switzerland Poland Austria Sweden Finland Benelux Portugal Romania Japan Philippines Singapore Malaysia Australia China South Korea New Zealand