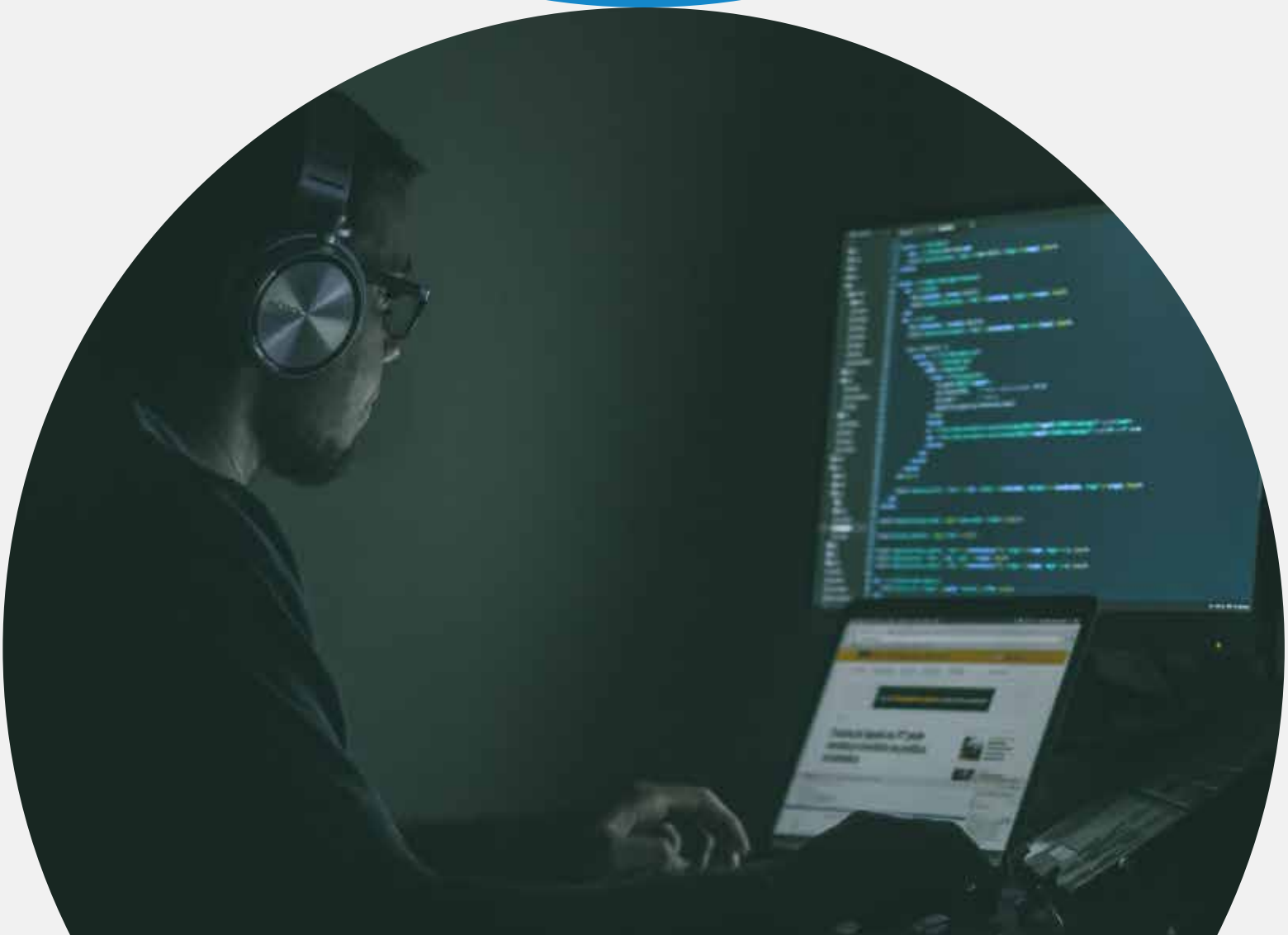
US President's Executive Order on Improving National Cybersecurity



The Executive Order – Key Takeaways

Public and private sector organizations in the US are under attack by nation states and cyber criminals using increasingly sophisticated and malicious activities. Cases such as the Solar Winds, Colonial Pipelines, and Microsoft Exchange point to a need to improve cyber defenses, protect public and private sector entities and the American people's security and privacy.

On 12th May 2021, the US President signed an executive order that covered three key areas to improve national cybersecurity:

Improve software supply chain security by establishing baseline security standards

- Remove barriers to sharing information on cyber threats and incidents on Federal systems.
- Increase collaboration between service providers and Federal agencies during investigation of incidents or potential incidents.
- Maintain greater visibility into their software and make security data publicly available.

Modernize and implement stronger cybersecurity standards

- Cloud service governance framework for secure cloud services.
- Implement zero trust architecture.
- Mandate deployment of multifactor authentication and encryption of data at rest and transit.

Improve the Federal Government's investigative and remediation capabilities

- Threat information sharing between the government and the private sector.
- Standard playbook for responding to cyber incidents.
- Cybersecurity Safety Review Board, co-chaired by the government and private sector leads.
- Endpoint Detection and Response (EDR) deployment.

Key Considerations for a New Reality

For effective implementation of policies, frameworks, standards and guidelines that will be formulated as part of the execution of the order, the top management should seek answers to key questions in each of the three areas in order to understand their current state and the gaps:

Software Supply Chain Security

- What are the critical business processes across the supply chain?
- Do we know how our suppliers and partners are managing cyber supply chain risks for the products and services we acquire?
- How do we ensure that the vendors stay current on emerging vulnerabilities? What are the vendor capabilities to address new "zero day" vulnerabilities?
- Is the vendor's software / hardware design process documented? Is it repeatable & measurable?
- How do we continuously monitor supply chain processes for compliance to standards and address issues?
- How do we ensure that suppliers communicate threats and vulnerabilities and mitigation actions, and regularly update on the status?

Modernize Cybersecurity

- Have we deployed inventory of cloud services?
- How do we ensure that service providers comply with the cloud-services governance framework?
- How do we assess or implement zero-trust architecture when migrating to cloud technology?
- How do we identify requirements and adopt multi factor authentication and encryption of data?
- How and when do we assess the security of cloud services?
- How do we monitor, identify, and quickly respond to emerging cyber threats and prevent cyber incidents?

Improve Cyber Defense

- How do we identify cyber vulnerabilities and defend our system and functions from cyber incidents?
- How do we ensure we have created a threat database, kept it current and shared it with other government agencies and departments?
- How do we effectively implement the playbook to respond to cyber incidents and provide information to the Cyber Safety Review Board if an incident occurs?
- How do we incorporate cyber resilience in the fabric of digital care and data privacy elements?
- How is cyber risk management integrated into procurement and the day to day operations process?
- How do we improve our detection, analysis and response capabilities towards cyber incidents?

Need for real-time visibility into cybersecurity posture to move the perspective from hindsight to insight and foresight

Strategies to Improve Cybersecurity Posture

Consider developing a strategy that helps close the gaps identified in your supply chain security, the current cybersecurity structure, and cyber defense mechanism. People, process, and technology, play a critical role in building cyber resilience and improving your cybersecurity posture. Following are the points you could consider:

Improve supply chain security and mitigate supply chain attacks

- Develop effective policies and procedures for usage of third-party applications, cloud services, and personal devices.
- Audit 'Shadow IT' infrastructure to mitigate 'Shadow IT' risks.
- Identify, establish, assess, and manage Software Supply Chain Risk Management processes. Leverage contract clauses to ensure that software suppliers implement appropriate safeguards to meet the objectives of an organization's cyber program.
- Establish solid third party governance by creating effective policies and procedures for supplier on boarding, classification and profiling, supplier assessment, relationship monitoring, and relation severance.
- Develop processes and methodologies for continuously monitoring third parties based on risks, leveraging technology solutions.

Modernize and implement stronger cybersecurity standards

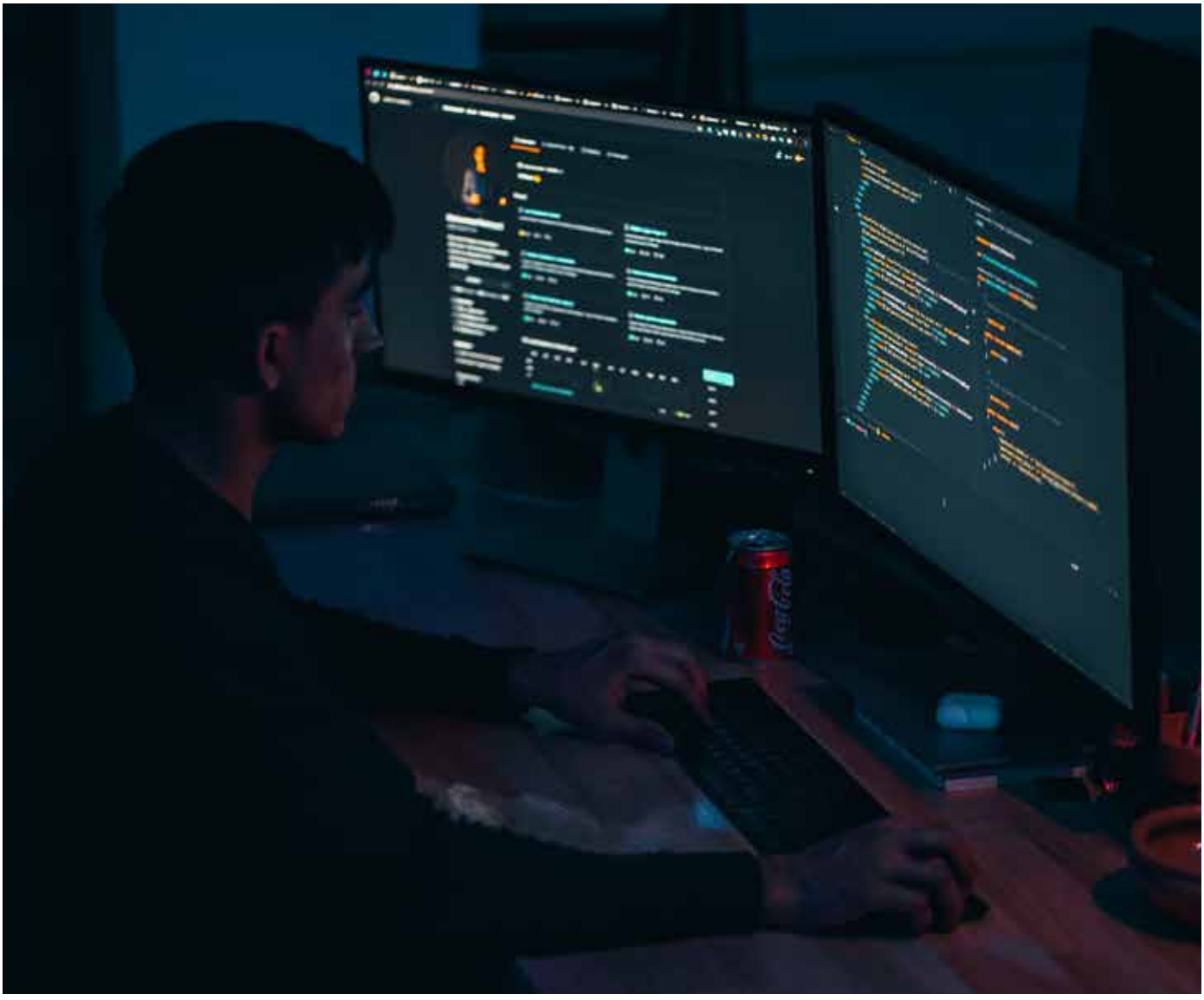
- Establish a cloud service governance framework for securing cloud services covering the cloud operation center, protection of information during transit and rest, protection of cloud infrastructure and applications, and the implementation of secure identity and access management.
- Conduct Threat Modelling based on the known vulnerabilities pulled from authoritative sources, understanding business needs, security operations, and the various compliance requirements.
- Conduct Security Architecture Assessment covering security operations layer, data management layer, application layer, information transfer layer.
- Enforce Multi-factor authentication using advanced secure, password-less authentication services implemented across the organization for secure access of data that's stored and processed on cloud.
- Discover and classify data, implement DLP, anonymize data where possible, encrypt data, implement strong data governance frameworks, monitor and manage data.
- Implement Zero Trust Architecture using Continuous Adaptive Risk Assessment.
- Develop strategies to enhance the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources.
- Build secure software update processes as part of SDLC by adopting a builder and breaker strategy. Consider runtime application self-protection (RASP) and other client-side protection tools.

Strengthen cyber defense

- Forensically analyze incidents to improve investigative and remediation capabilities.
- Develop Framework for Threat Information Sharing between the government and the private sector.
- Deploy EDR to promote active cyber hunting, containment, response, and remediation.
- Standardize playbooks to respond to cyber incidents and automate breach notification.

Contact us:

Reach out to us at **cybersecurity.services@wipro.com** for more information.



Wipro Limited
Doddakannelli,
Sarjapur Road,
Bangalore-560 035,
India
Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 200,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information,
please write to us at **info@wipro.com**

IND/BRD/AUG2021- JUL2022