The Statesman

11 April, 2018

'Framework should be set up to curb cyber incidents'

IANS
NEW DELHI, 10 APRIL

An Assocham-PwC joint paper on Tuesday said a framework should be established to effectively curb cyber incidents and reduce the time taken in responding to them.

The paper highlighted the need for seamless flow of information between state intelligence agencies, central intelligence agency, various government departments and ministries in the country. It also recommended that the government, industry and security vendors should come together on a common platform to formulate and implement policies and procedures for cyber security.

The joint paper was prepared by industry lobby Assocham and consulting firm PwC based on post-event recommendations for Assocham's 10th annual summit on cyber and network security submitted to the government.

The paper said the Union government must set up a central security operations centre (SOC) with advanced analytical capabilities to enable continuous and real-time monitoring of all information technology (IT) assets, interconnected networks and operational environments.

"The SOC should develop a fusion centre to integrate information available from other commercial sources as well to have a better assessment of evolving global threats," said the paper.

"The government should consider active participation in international cyber security conventions and treaties, which provide measures to combat cybercrime and gather electronic evidence from service providers," it added.

With a view to establish programmes to promote research and development (R&D) in the field of cyber security, the paper suggested the government to introduce tax incentives, subsidies and investment funds, and also set aside a budget for every cyber security-information and communication technology (ICT) project on the lines of Singapore which was ranked on top in cyber security index released by the UN in June 2017.

The Assocham-PwC paper said the government should carry out due diligence and accordingly prescribe baseline cyber security parameters for relevant systems to be deployed in the government ecosystem as well as for critical information infrastructure protection.

"The emphasis should be on building capabilities and capacities for application, equipment and infrastructure testing through deployment life cycle to detect and mitigate any vulnerabilities and backdoors in the product/technology," it added.

Telangana Today (Hyderabad) 11 April, 2018

'Framework on cyber security is needed'

Assocham says it is time to establish security operations centre

BUSINESS BUREAU
Hyderabad

NEED OF THE HOUR: *The SOC, according to the paper, will enable continuous and real-time monitoring of all IT assets.*

With the increasing incidents of cyber-attacks, it is becoming inevitable to create infrastructure that ensures cyber security to protect critical assets. Emphasising the need for keeping security mechanism in place, apex industry body Assocham has appealed to the Central government that it must set up a central security operations centre (SOC) with advanced analytical capabilities to enable continuous and real-time monitoring of all information technology (IT) assets, interconnected networks and operational environments.

"The SOC should develop a fusion centre to integrate information available from other commercial sources as well to have a better assessment of evolving global threats," noted a joint paper prepared by Assocham and consulting firm PwC based on post-event recommendations of Assocham's 10th annual summit on cyber and network security. The paper recommended that all the stakeholders-government, industry and security - must come together on a common platform to formulate and implement policies and procedures for cyber security.

It also highlighted the need for seamless information exchange among State intelligence agencies, Central intelligence agency, varto cyber incidents, it noted. India should ensure active collaboration with other countries and global cyber security agencies through international treaties, bilateral agreements and memorandums of understanding to understand the latest threats and take proactive measures to tackle them.

With a view to establish programmes to promote research and development (R&D) in the field of cyber security, the paper suggested the government to introduce tax incentives, subsidies and investment funds. Government should also set aside a budget for every cyber security-information and communication technology project on the lines of Singapore which is ranked on top in cyber security index released by the UN in June 2017.

Government should carry out due diligence and ac-

The joint paper by Assocham and PwC called for budget allocation for every cyber security ICT project

tection. "The emphasis should be on building capabilities and capacities for application, equipment and infrastructure testing through deployment life cycle to detect and mitigate any vulnerabilities and backdoors in the product/technology."

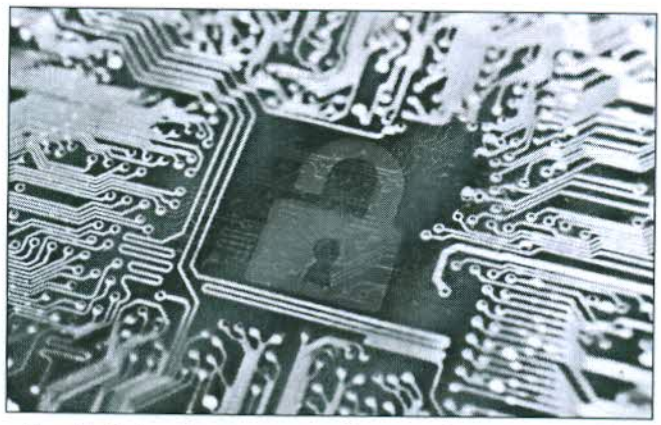
The paper also pointed out that there is a need to promote cyber security as a skill set. Government should include cyber security related skills in the job descriptions of government employees by working in close co-ordination with Department of Personnel

Central Chronicle 11 April, 2018

Cyber Incidents: ASSOCHAM-PwC Joint paper suggests govt to set up SOC

Agencies, Hyderabad

The Union government must set up a Central Security Operations Centre (SOC) with advanced analytical capabilities to enable continuous and real-time monitoring of all information technology (IT) assets, interconnected networks and operational environments to curb Cyber incidents, suggested an ASSOCHAM-PwC Joint paper.



"The SOC should develop a fusion centre to integrate information available from other commercial sources as well to have a better assessment of evolving global threats," noted a joint paper prepared by ASSOCHAM and consulting firm PwC based on post-event recommendations for ASSOCHAM's 10th annual summit on cyber and network security submitted to the government. In its paper , the Industrial body recommended to the government that industry and security vendors come together on a common platform to formulate and implement policies and procedures for cyber security, ASSOCHAM said in a release here on Tuesday.

Highlighting the need for seamless flow of information between state intelligence agencies, central intelligence agency, various government departments and Ministries in India, the paper also said that a framework should be established to effectively curb cyber incidents and reduce the time taken in responding to it It also suggested that India should ensure active collaboration with other countries and global cyber security agencies through international treaties, bilateral agreements and memorandums of understanding in order to understand the latest threats and take proactive security measures to tackle them. "The government should consider active participation in international cyber security conventions and treaties, which provide measures to combat cybercrime and gather electronic evidence from service providers," It said. With a view to establish programmes to promote Research and Development (R&D) in the field of cyber security, the ASSOCHAM-PwC paper also suggested the government to introduce tax incentives, subsidies and investment funds.

Sikkim Express 11 April, 2018

'Framework should be set up to curb cyber incidents effectively'

NEW DELHI, April 10 (IANS): An Assocham-PwC joint paper on Tuesday said a framework should be established to effectively curb cyber incidents and reduce the time taken in responding to them.

The paper highlighted the need for seamless flow of information between state intelligence agencies, central intelligence agency, various government departments and ministries in the country.

It also recommended that the government, industry and security vendors should come together on a common platform to formulate and implement policies and procedures for cyber security.

The joint paper was prepared by industry lobby Assocham and consulting firm PwC based on post-event recommendations for Assocham's 10th annual summit on cyber and network security submitted to the government.

The paper said the Union government must set up a central security operations centre (SOC) with advanced analytical capabilities to enable continuous and real-time monitoring of all information technology (IT) assets, interconnected networks and operational environments.

"The SOC should develop a fusion centre to integrate information available from other commercial sources as well to have a better assessment of evolving global threats," said the paper.

"The government should consider active participation in international cyber security conventions and treaties, which provide measures to combat cybercrime and gather electronic evidence from service providers," it added.

With a view to establish programmes to promote research and development (R&D) in the field of cyber security, the paper suggested the government to introduce tax incentives, subsidies and investment funds, and also set aside a budget for every cyber security-information and communication technology (ICT) project on the lines of Singapore which was ranked on top in cyber security index released by the UN in June 2017.

The Assocham-PwC paper said the government should carry out due diligence and accordingly prescribe baseline cyber security parameters for relevant systems to be deployed in the government ecosystem as well as for critical information infrastructure protection.

"The emphasis should be on building capabilities and capacities for application, equipment and infrastructure testing through deployment life cycle to detect and mitigate any vulnerabilities and backdoors in the product/ technology," it added.

Highlighting the need for the government to focus on promoting cyber security as a skill set among individuals, the paper said that government should include cyber security-related skills in the job descriptions of government employees by working in close co-ordination with Department of Personnel and Training (DoPT).

It added that including cyber security in educational programmes and promoting it as a mainstream profession would help the sector attract right talent.

The paper further said that the government should also grant security clearances and non-disclosure agreements (NDAs) to third parties and vendors working for critical establishments.

The Assocham-PwC joint paper also said that the government should define a national cyber security awareness programme — identifying the target audience and defining mechanism to disseminate cyber awareness material effectively — and introduce cyber security courses at all levels of education such as undergraduate school and panchayat levels.