Protecting Critical Infrastructure and Systems of National Significance

Industry Consultation

Cybersecurity & Risk Services
WIPRO LIMITED | LEVEL 17, 201 MILLER STREET, NORTH SYDNEY, NSW - 2060, AUSTRALIA

Executive Summary

Wipro appreciates the opportunity to participate in this Cyber Security Industry Sector Consultation initiative sponsored by the Australian Government as it considers its approach for protecting Critical Infrastructure and Systems of National Significance.

We have been supporting the security services needs of our clients in Australia, across both corporate and government sectors for the past 15 years. Based on this experience, we have gained a significant level of insight into the maturity of the practices as well as the supporting governmental eco-system which enables Agencies to design, operate and proactively manage a cyber-resilient ecosystem.

We are delighted to contribute our insights in the areas where we have our strengths backed by relevant experience. We hope the information shared helps to shape the Australian Government Cyber Security Strategy with regards to protecting critical national infrastructure and systems of national significance and would welcome the opportunity to engage in any follow-up workshops, focus groups and strategy consultation support to turn early stage strategic visions into reality. Accordingly we would commend to the Australian Government the following vision and component delivery objectives:

Vision	
"By 2024, the Australian Government should have established a cyber-physical resilient ecosystem for critical infrastructure, systems and digital assets of national significance which encourages proactive threat identification and reduction with integrated response plans defined and tested on a regular basis and the sharing of appropriate threat intelligence."	
Critical Objectives	
Objective 1 – Establish a comprehensive inventory of critical infrastructure assets on a sector by sector basis	**Objective 2 –** Establish a comprehensive threat inventory for the assets identified as part of Objective 1 to establish the national infrastructure attack surface.
Objective 3 – Actively participate and monitor the reduction of vulnerabilities in critical assets and also in organisational networks and systems in the pursuit of a converged state where Enterprise IT, OT, IoT reside at equivalent levels of maturity with a 'single pane of glass view' in a consolidated and converged Industrial Internet of Things (IIoT) environment and risks are mitigated based on an agreed risk based assessment model.	**Objective 4** – The Australian Government should build upon existing Australian Cyber Security Centre (ACSC) and Joint Cyber Security Centre (JCSC) initiatives, leveraging Australian Signals Directorate (ASD) and Australian National Cyber Security Strategy to establish a member driven government enabled collaborative ecosystem to tackle cyber disruption thus enabling Australia to be one of the most secure places in the world for critical infrastructure and systems of national significance.

Background & Situational Requirement

The world is undergoing a period of unprecedented challenge and whilst this has impacted economies both globally and locally, it is inevitable that as the world recovers from the COVID-19 pandemic crisis, both nations and organisations will recognise opportunities to enhance their technological landscape to develop a new more-virtual operating norm and to uplift their cyber resilience as part of any transformative activity.

With the current proliferation of Operational Technology (OT) and the increased adoption of Internet of Things (IoT) expected in the near future, there is an urgent need to adopt security good practices within the realm of OT and IoT equivalent to those currently emphasised in Enterprise IT in order to achieve security convergence. These good practices need to extend both into 'protect' as well as 'detect & respond' security controls and can be delivered through the establishment of a centrally coordinated information sharing partnership with centralised dark web monitoring and intelligence capabilities open to all member organisations.

Operational Technology (OT) encompasses hardware and software that monitors and manages physical equipment and processes. It includes a variety of Industrial Control Systems (ICS) such as Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) systems and Internet of Things (IoT) connected devices which are now increasingly referred to as the "Industrial Internet of Things" (IIoT).

As the use of OT, IoT and in turn IIoT, increases, the need to secure these technologies has never been more important. They are often business critical in many industries and examples include the monitoring and control of core infrastructure such as oil and gas drilling and distribution; energy generation and distribution; chemical, pharmaceutical and consumer goods manufacturing; and increasingly health, building management, transportation and telecommunications applications, among others. Failure directly affects business operations and revenue and in some cases safety as well.

Because they run essential systems in critical infrastructure and deliver responsive capabilities in real-time (such as meeting surge demand / usage). OT networks need to be operational at all times), so unlike other industries where Confidentiality is key, Availability is now the primary security concern.

The traditional approach to securing OT networks has involved leveraging air gaps or creating physical separation from IT networks in order to isolate them from cybersecurity risks. OT networks were presumed to have a reduced risk profile with respect to cyberattacks due to the difficulty in developing attacks for proprietary protocols and archaic technology. However, in a digitally-connected age where technological advances are continuing apace, these traditional safeguards have all but disappeared. In the last 20 years, OT has been exposed directly to outside risks via remote sensors to retrieve data, Wi–Fi–enabled controllers and USB devices to update software, for example. Additionally, we note that many producers are starting to market cloud–based "SCADA–as–a–service" platforms.

The driving principle for our recommended objectives is the provision for and the maintenance of societal need; given the generally accepted 5 stages of societal breakdown and resilience, with any significant unresolved disruption to critical infrastructure or critical services potentially triggering the *'Anarchy'* stage anytime between 72 hours to 2 weeks after the event.

As government and enterprises alike transform technology landscapes through widespread adoption of cloud, digitisation of services and smart operations enabling Industry 4.0; this presents the Australian Government the opportunity to establish and deliver a progressive and forward thinking cyber security strategy targeting an accelerated economic transformation that shapes a new digitally based economy underpinned by cyber-resilience.

Wipro considers that role of the Australian Government is to provide a safe, secure and resilient cyberspace for critical infrastructure and systems of national significance to ensure the continuous availability of services for its citizens, businesses and machinery of government. To this end, all parties can be both providers and consumers of each other's services although Australian Government should play a central coordination role in the creation/enhancement of the Australian Government's digital resilience. Therefore, Wipro suggests that the Australian Government should focus on three core outcomes, specifically:

1) Protection of critical state assets (not just information) and services from cyberattack.
2) Provision of a focal point for cyber security incident management for events that have an impact at a state or national level.
3) Provision of resources and education to improve and uplift the overall security of critical infrastructure through technical solutions as well as providing guidance to citizens and businesses.

At Wipro we therefore believe that core to Australian Government's cyber strategy development for protecting Critical Infrastructure and Systems of National Significance should be the recognition that to support such a transformation, the Australian Government should embrace a vision that:

"By 2024, the Australian Government should have established a cyber-resilient ecosystem for critical infrastructure and systems of national significance which encourages proactive threat identification and reduction with integrated response plans defined and tested on a regular basis and the sharing of appropriate threat intelligence."

In terms of campaigns, Wipro would suggest keeping the message simple with little technical language and in terms of measures – increased enforceable accountability would be strongly recommended. Whilst many governments have stopped short of legislative mandate there are increasing trends to incentivise increased cybersecurity through common criteria and corporate governance as well as minimum criteria for government supply chain contracts

Proposed Strategic Objectives

To enable this vision, based on our collective corporate and client experience, we have identified the following critical pragmatic steps as delivery objectives to enable the Australian Government to successfully deliver upon this vision:

Objective 1

Establish a comprehensive inventory of critical infrastructure assets on a sector by sector basis

One of the main cybersecurity challenges that CIOs and CISOs are being tasked to address is:

- Limited visibility and insight. Propriety protocols in OT make it difficult, if not impossible, for IT solutions to map the attack surface. IT security solutions, for the most part, have not been adapted to work in OT environments. For example, permissive scanning is generally prohibited, leaving these areas in the dark for vulnerability management practices, risk awareness and proactive threat protection.

While the convergence of IT and OT technologies is creating tremendous productivity benefits, it is also introducing new security risks. In fact, nation–state cyber warfare, led by bad actors in search of political power and financial gain, has already carried out multiple successful attacks. Ransomware infections in 2017, including WannaCry and NotPetya, showed the threat to converged networks.

IT systems connected through poorly configured networks to OT systems running unpatched operating systems can massively disrupt OT systems, bringing production lines to a halt and general business operations to a standstill. Given their criticality, disrupting OT systems and assets can have disastrous outcomes including accidents and injuries, loss of life, environmental disasters, interruption in vital services and the associated economic losses.

Threats to OT are difficult to fight because of all of the challenges cited above and because standard security measures in IT networks often do not work with OT environments.

As an example, patching vulnerabilities on OT devices requires downtime that is not always possible and can actually crash devices as well as invalidate their vendor support.

However, the biggest challenge organisations are struggling with is visibility of the IT–OT attack surface.

Visibility is essential in security to understand the environment and its connections, design security architectures, identify attack vectors and locate blind spots, among other things. Without visibility, unknown and unchecked security issues abound including access policy violations, vulnerabilities, misconfigurations, faulty design in the form of weak security controls as well as unplanned or unauthorised changes. While there may be visibility solutions for IT and OT networks individually, they rarely intersect. Manually piecing together information from such solutions can be imprecise and gaining contextual intelligence from them is an even bigger task. With teams already overloaded, this becomes an impossible situation.

On the OT side, discovery should be conducted by passively collecting information about OT network assets and network topology using accredited OT security sensors to identify:

- Devices of the DMZ (firewalls and any other security controls)
- Level 3 control system LAN, with assets such as manufacturing systems, inventory control and any routing equipment
- Level 0–2 assets, including information about the type and location of field devices, PLCs and other machines

It is critical to underline that the approach to this information collection needs to be completely passive. This is because OT networks are impossible to actively scan - both because of time requirements and because of certification issues.

Objective 2

Establish a comprehensive threat inventory for the assets identified as part of Objective 1 to establish the national infrastructure attack surface.

Once a comprehensive inventory of OT assets has been completed, the challenge that poses itself is how to categorise, impose and maintain the fundamental security measures on OT. We believe that the following list captures the types of challenge that are pertinent to OT as opposed to Enterprise IT, specifically:

- Legacy technology: OT is rife with legacy technology designed long before the advent of security measures common today, such as encryption or password protection. Even though these systems are not secure, they are kept up and running as long as they remain operational. Even if an organisation wanted to switch out their OT, there may be no better option on the market. Poor security, including weak passwords (for example, "password") can also be embedded at the firmware level and are, therefore, unchangeable.
- Outdated systems: The firmware itself can also be outdated, such as in PLCs, with no update process in place, leaving them vulnerable. Therefore, when security measures are installed on IT assets within the OT network, these IT assets are often outdated systems with known vulnerabilities in the software stack that may or may not have vendor support to fix them. For example, old Windows machines that are no longer supported by Microsoft - as an example, Windows XP is still widely used within OT environments.
- Non-secure connections: To easily transfer control data or use new applications, OT devices communicate with the IT network or laptops, or use USBs. Sometimes this communication is performed over unencrypted Wi–Fi connections, leaving them vulnerable to man– in–the–middle attacks.
- Convergence with IT: As OT connects with the corporate network, it also becomes vulnerable to malware and vulnerabilities as well as malicious insiders. In addition, as OT systems become smarter and more IT–enabled, OT engineers are tasked with adding IT knowledge and security expertise to their already full and distinct workloads and are being expected to adopt wider cybersecurity governance regimes. Conversely, IT teams are not typically well–versed in OT systems, concerns and protocols, creating a clash of cultures and experience in tackling technology security challenges.
- Organisational challenges: Because IT and OT each have different teams, technologies, processes and objectives, it is difficult to create and maintain security architectures that meet the needs of both groups. This security management disconnect also creates cracks which attackers can take advantage of to move throughout the organisation.

Wipro suggests that to manage security across traditionally disparate IT and OT environments, organisations must be able to see and understand the entire attack surface of their technology landscapes, including physical IT and OT, virtual and multi–cloud networks. Illuminating the entire context of the network provides a better, more complete foundation to understand risks anywhere in the organisation.

Once the attack surface has been defined as the sum total of all the ways in which a network is vulnerable to cyberattack it becomes possible to plan a remediation strategy. Wipro notes that ab attack surface generally consists of the network topology, security controls and assets in the IT and OT environments, as well as the security issues, vulnerabilities and threats that put them at risk.

OT attack vectors include:

- Lateral movement through corporate networks, made possible by IT–OT convergence
- Infiltration via remote access and/or spear-phishing (advanced persistent threats)
- Direct access from disgruntled employees as well as external contractors and other third parties such as suppliers and support vendors
- Malware injected through internet connections or direct access
- Targets such as HMI interfaces, DCSs, PLCs, and RTUs
- Malfunctioning units, unmapped networks and configuration mistakes

Building the optimal attack surface visibility typically involves an automated four–step method of: discovery, modelling, analytics and visualisation.

Objective 3

Actively participate and monitor the reduction of vulnerabilities in critical assets and also in organisational networks and systems in the pursuit of a converged state where Enterprise IT, OT, IoT reside at equivalent levels of maturity with a 'single pane of glass view' in a consolidated and converged Industrial Internet of Things (IIoT) environment and risks are mitigated based on an agreed risk based assessment model.

Once a unified and convergent view of the attack surface across the entire environment helps organisations:

- Understand network context with holistic network modelling and mapping:
  - All routing paths on the networks
  - Device and configuration checks (hardening)
  - Dynamic access analysis (processing LAN/ corporate LAN/engineering P2P network)
  - Communication discovery between OT assets (ISA99/IEC62443 level)
- Confirm effective controls through firewall and access control analysis:
  - Policy compliance (e.g., for NERC, FISMA, NIST, ISA99/IEC62443 level)
  - Platform security
  - IPS analysis
  - Ruleset clean-up and optimisation
  - Secure change management
- Identify vulnerabilities and prioritise patching with complete context:
  - Centralised vulnerability data from active and passive discovery methods across your entire network
  - Intelligent remediation prioritisation identifying exposed vulnerabilities and those exploited in the wild
  - Prioritised patching process
  - OS and protocol–based risk assessment
  - Identification of compensating controls when patching isn't an option

Furthermore, it allows risk to be addressed based on highest priority first. In a converged IT–OT environment, it is critical to understand how vulnerabilities affect risk levels of the entire organisation to accurately establish and set remediation priorities.

To do so requires risk-based vulnerability management. This approach takes into account all an organisation's vulnerabilities, correlating them with the network model and real–time threat intelligence to determine which vulnerabilities are most likely to be used in an attack.

With this information, security programs can accurately prioritise remediation to ensure critical patches are applied during scheduled OT downtime or compensating controls can be put in place until such time.

Wipro proposes that that a Risk-based vulnerability management should consider:

- The criticality of vulnerabilities
  - CVSS score
  - Potential exploitation impact
- The context of vulnerabilities, including asset criticality and exposure
  - Internet or third–party access
  - Business value and data sensitivity
  - Surrounding network topology and security controls
- The assessment of the threat
  - Active exploitation in the wild
  - Availability of sample exploit code
  - Used in malware, exploit kits, etc.

Objective 4

Australian Government should build upon existing ACSC and JCSC initiatives, leveraging ASD and Australian National Cyber Security Strategy to establish a member driven government enabled collaborative ecosystem to tackle cybercrime enabling Australian Government to be one of the most secure places in the world to do business by establishing an enhanced cyber information sharing partnership platforms to enable the digital economy to operate as a cohesive ecosystem capable of collaboratively repelling cyber criminality and preserving societal digital trust across Australian Government.

The creation of a secure critical national infrastructure ecosystem places an ever increasing reliance on the timely delivery and action of threat intelligence. Traditional routes see individual organisations focus on protecting their individual information and cyber physical assets, but when considering more forward thinking cybersecurity, a different approach is required.

To this end we would recommend that Australian Government further enhance existing initiatives to deliver a "Cyber information Sharing Partnership" acting as a collaboration of member organisations with a single common intent – the prevention or minimisation of cyber-crime.

Unlike many aspects of technology, organisational attitudes to cybercrime recognise that organisations in the public sector, private sector and broader society are aiming to protect themselves against a common threat and accordingly there is a greater willingness to share information beyond organisational boundaries to enable organisations of all sizes to be aware of threat intelligence and protect themselves from known Indicators of Compromise (IOC).

Such a platform should be enabled and administered by Australian Government with organisations committing to providing a minimum volume of resource support (in the case of large enterprises) and open access to timely sharing of information, albeit such information could be provided in an anonymised manner.

To amplify such information sharing Australian Government could commission and procure support from specialised cybersecurity providers such as Wipro to enable such a platform and provide otherwise unavailable insight such as access to IOC databases and dark web threat intelligence analyst, which could be provided to larger organisations on a chargeback model and smaller organisations on an altruistic basis by Australian Government.

Conclusion

Government and Businesses will continue to expand the connectedness of OT systems. Being able to read, reach, update, adjust or control OT systems from anywhere has significant business value. Nevertheless, these advantages come at a cost and those responsible for security in IT–OT networks need to have the right security tools to fit the unique needs of the security challenge at hand.

A unified approach to IT–OT security management based on model–driven, comprehensive visibility gives organisations:

- Non–intrusive security oversight of production networks to minimise downtime
- Contextual understanding of risk throughout the entire IT–OT environment
- Improved communication between IT and OT security stakeholders via a common and complete view of the attack surface

The adoption of a unified approach dissolves the traditional organisational challenges between IT–OT teams, so that OT engineers can focus on maintaining services without becoming security experts, and IT security has the insight they need to effectively understand and manage risk.

Contributors

Mark Brown
Partner - Global Head OT & IoT Security

- Mark has extensive international and sectoral experience across many facets of technology leadership and has previously been a global FTSE 10 Consumer Goods CISO, global FTSE 150 Manufacturing Sector CIO and for 4 years led EY's UK & Ireland Cybersecurity advisory and assurance consulting practice.
- Mark's experience in global IT strategy and digital transformation, cybersecurity and IT risk management and the application of enterprise wide cyber risk models enables him to provide insightful, pragmatic advice to his clients on the paradigm of right-sizing Cybersecurity and wider IT risks within business as a strategic enabler rather than a compliance focused inhibitor.

Mark can be contacted at [redacted]

Justin Parr-Davies
Partner - APJ Head OT & IoT Security

- Justin has worked globally across a number of industry sectors including Energy and Utilities, Engineering as well as Banking and Financial Services in a number of leadership roles and has previously served as Chief Information Security Officer for a Victorian Statutory Authority and the Global Head of Technology Governance, Risk and Assurance at a Global Energy and Resources organisation.
- Justin's broad experience in IT / OT / IoT Strategy Governance, Compliance, Cybersecurity, Risk Management and Assurance underpins his ability to provide practical advice to his clients on Cybersecurity matters and the broader domain of IT / OT and IoT Risk.

Justin can be contacted at [redacted]

[redacted]

Addendum 1

In the table below, please find some general information about Wipro:

Corporate Information

Information	Response
Name of Business	Wipro Limited
Contact for further queries	
Number of employees (total)	Wipro currently has over 187,000 employees distributed across 59 countries supporting 1070 active global clients.
Number of employees in cyber security roles	Based on FY 20 Wipro has 9,293 employees in cyber security roles globally
Annual turnover of business ($, total)	$ 8.2 Billion USD
Annual turnover of business ($, cyber security activities)	Annual turnover was 433.0 Mn USD globally for cyber security
Do we export cyber security services/products?	Yes, Wipro is one of the largest cyber security services provider globally
If so, what proportion of cyber security turnover is attributable to exports?	93.8% of total revenue is from global cyber security engagements
Specific area of cyber security expertise	1) Network security 2) Endpoint and mobile security 3) Identification, authentication and access controls 4) Operational security management 5) Information risk assessment and management 6) Assurance, audits and compliance 7) Implementing secure systems, including consulting on adoption of secure SDLC, DevSecOps 8) Threat intelligence, monitoring, detection and analysis 9) Incident response and management 10) Securing Operational Technology, ICS, SCADA, Critical Infrastructure and Internet of Things (IoT) 11) Security awareness, training and education 12) Security platforms research and development 13) Managed Security Services including Security orchestration & automation 14) Cyber security and resilience consulting 15) Enterprise Risk Management
Which industry sectors are our main customers?	The market segments in which Wipro operates are described internally as 'strategic business units' or 'verticals' and are specifically: 1) Banking, Financial Services and Insurance 2) Communications 3) Public Sector, Retail and Consumer Packaged Goods 4) Energy, Resources, Utilities and Construction 5) Healthcare and Life Sciences 6) Manufacturing 7) Technology (Platform and Products)
What percent of our staff do we expect to leave our company in next 2 years?	**14%**
To what extent on a scale of 0 (low) - 5 (high) are we able to meet your cyber security skills needs with staff from the Australian labour markets?	**3**

Information	Response
Technical cyber skills we consider lacking in our business or amongst job candidates?	While we have developed robust processes to groom security talent internally with our organisation, we find it difficult to source below skills locally in Australia, although it is recognised that these are premium skills with a shortage of available talent (at reasonable costs): - Threat detection and response; - Threat intelligence analysts; - OT / ICS security SMEs; - Certified ethical hackers; - Experienced secure SDLC/DevSecOps SMEs;