Strengthening Australia's cyber security regulations and incentives

Authors: Justin Parr-Davies, Ganesha Rajanaidu & Vrinda Muzumdar

Date: August 2021

Public

Introduction

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 strengthening Australia's cyber security regulations and incentives for sectors not covered by the proposed amendments to the Security of Critical Infrastructure Act 2018 and around connected devices or the Internet of Things (IoT).

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 underlying governance eco-system.

We are delighted to contribute our insights in the areas where our consulting strengths are backed by relevant practical implementation experience. We hope the information shared helps to shape the Australian Government Cyber Regulations and Incentives Strategy with regards to developing a proactive regulatory environment and we 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 propose supporting the Australian Government's 2020 Cyber Strategy's vision with four (4) component delivery objectives:

Australian Government's 2020 Cyber Strategy Vision	
A more secure online world for Australians, their businesses and the essential services upon which we all depend.	
Key Objectives	
Objective 1: Defined a consistent but flexible approach that balances technological innovation with the need for increased levels of security for IoT devices and 'end-to-end' personal data protection.	**Objective 2:** Defined a set of baseline standards aligned to those that are already internationally accepted such as National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF), ISO27001 and European Telecommunications Standards Institute (ETSI) EN 303 645.
Objective 3: Established a labelling system equivalent to the UK's 'Kitemark' scheme to provide Australian consumers a clear indicator of an IoT product's or an organisation's level security and privacy to enable consumer confidence.	**Objective 4:** Established and appropriately empower a body to assess compliance with the mandatory set of baseline standards to provide ongoing assurance to the Australian consumer and to address any areas of non-compliance with measurable action plans. It should assess and validate the remediation of higher risk vulnerabilities that have been identified to reduce potential harm.

Chapter 2: Why should government take action?

Objective: Action by Government to rebalance the short-term value equation to allow organisations to proactively address negative externalities and information asymmetries in cyber security.

Consultation Q1: What are the factors preventing the adoption of cyber security best practice in Australia?

Our experience working with large companies (e.g. ASX Top 50) and not for profit organisations highlight factors preventing the adoption of cyber security good practice in Australia are well known and this includes:

- Weak short-term incentives as most companies are designed to maximise shareholder value
- Lack of cyber regulations (exceptions are Australian Prudential Regulation Authority's (APRA's) CPS-234 for financial services and Australian Energy Market Operator's (AEMO's) Australian Energy Sector Cyber Security Framework (AESCSF) for the energy sector)
- Weak enforcement (e.g. AEMO's AESCSF) or the lack of expected outcomes (e.g. APRA's CPS-234) where there are regulations
- Board composition with limited technical knowledge impedes effective risk management
- Lack of cyber leadership with most companies not having a Chief Information Security Officer (CISO) and if a CISO is available, in most cases they report to Chief Information Officers (CIOs) which is a conflict of interest and thus impedes effective cyber risk management and allocation of resources.

Consultation Q2: Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

Yes, and it is the premise for our objective for this chapter as capital market economies like Australia lack inherent incentives to address negative externalities and information asymmetries as it reduces shareholder value in most cases. This is an excerpt from a Harvard Business Review (HBR) article on shareholder value which encapsulates the typical decision-making process that results in the under investment in cyber security. "First, the accountant's bottom line approximates neither a company's value nor its change in value over the reporting period. **Second, organisations compromise value when they invest at rates below the cost of capital (overinvestment) or forgo investment in value-creating opportunities (underinvestment) in an attempt to boost short-term earnings**. Third, the practice of reporting rosy earnings via value-destroying operating decisions or by stretching permissible accounting to the limit eventually catches up with companies. Those that can no longer meet investor expectations end up destroying a substantial portion, if not all, of their market value"[1]. This model has no incentives to address externalities and therefore regulations and the cost of non-compliance is an opportunity for Government to help rebalance short term value equation to prevent underinvestment that has large negative externalities.

The case not to intervene would be the potential impact to shareholder value however the result can be a challenging operating environment as negative externalities and information asymmetries are not normalised. Ultimately this can have a negative impact to the ecosystem (citizens and businesses as a whole).

[1] https://hbr.org/2006/09/ten-ways-to-create-shareholder-value

Chapter 3: The current regulatory framework

Objective: Defined a set of baseline standards aligned to those that are already internationally accepted such as NIST CSF, ISO27001 and ETSI EN 303 645.

Consultation Q3: What are the strengths and limitations of Australia's current regulatory framework for cyber security?

In terms of strengths, foundational initiatives have kicked off for sectors of national critical significance with the amendments to the Security Legislation (Critical Infrastructure) Bill 2020, CPS-234 for the financial services sector and the AESCSF for the energy sector.

Inherent weaknesses for sectors not included in the critical infrastructure bill include:

- Lack of baseline standards
- Lack of enforcement
- Where voluntary self-assessments have been introduced, it has been found to be unreliable (e.g. CPS-234).

Consultation Q4: How could Australia's current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

Below is a summary of how we believe Australia current regulatory environment can evolve to provide:

- Clarity:
  - Development of minimum standards and guidance for sectors not included in the critical infrastructure bill
- Coverage:
  - We believe that coverage needs to be considered such that it does not impede on innovation and the start-up ecosystem. As such we recommend delineating organisations by type (e.g. B2B or B2C) and potential impact to citizens/residents and/or the economy
  - Thresholds should be set based on potential impact and obligation requirements should progressively increase accordingly. At lower thresholds obligations should be voluntary while at higher thresholds it should be mandatory (taking a risk-based approach)
- Enforcement:
  - Effective enforcement would require specialist skills in cyber security and given the limited availability of skilled resources, we recommend that enforcement be centralised. Centralisation would provide the scale to justify the investments required to be effective.

Chapter 4: Governance standards for large businesses

Objective: Defined a set of baseline standards aligned to those that are already internationally accepted such as NIST CSF, ISO27001 and ETSI EN 303 645.
Consultation Q5: What is the best approach to strengthening corporate governance of cyber security risk? Why?
We believe starting with a variation to Option 1. Specifically, regardless if standards are voluntary to begin, we recommend having mandatory requirements for cyber leadership (CISO role) and Board reporting requirements of this role for large organisations. Requirements should include no conflicts of interest in the reporting structure of the cyber leadership role. This should be a critical first step for all large businesses. We also strongly believe in learning from other people's experience. Voluntary schemes have historically had poor participation and limited outcomes. APRA's experience of rolling out CPS-234 also highlighted the fallacy of self-reporting schemes. Based on this experience, we recommend that the Government provides a high-level roadmap (e.g. over three years) to move from our proposed Option 1 strategy to Option 2 (mandatory baseline standards) for large businesses with large negative externalities. This we hope will provide the right balance by providing time for industry to understand standards, government to build regulator capabilities and forecast large investments.
Consultation Q6: What cyber security support, if any, should be provided to directors of small and medium companies?
The biggest issue for directors of small and medium sized companies is access to leaders with expertise in cyber security. We believe having a centralised advisory body that is easily accessible to company directors will help bridge expertise gaps at the top. Government should also consider public / private partnerships (e.g. with the AICD[2]) to develop relevant training and good practice guidance material for directors of small and medium sized businesses.
Consultation Q7: Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?
The threat landscape is ever evolving, and our business leaders need to keep up to pace. Awareness and training of senior business leaders should include: • Strategic up to date threat intelligence for their sector to obtain situational awareness • Industry cyber maturity benchmarks to compare against peers • Training on how to move from a compliance based to a risk based cyber management approach

[2] Australian Institute of Company Directors

- Information sharing within industry sectors (e.g. incidents and near misses).

Note, we believe that in large organisations it should be the CISO's role to translate the above cyber security context for senior business leaders and would be responsible for keeping them up to date by leading an effective cyber culture program. This becomes an increasing challenge for small and medium sized businesses. The centralised advisory function proposed in this chapter can be used to address some of these gaps.

Chapter 5: Minimum standards for personal information

Objective: Defined a consistent but flexible approach that balances technological innovation with the need for increased levels of security for IoT devices and 'end-to-end' personal data protection.
Consultation Q8: Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?
Establishing a cyber security code under Privacy Act, may result in application of cyber security controls restricted to personal information and not to all other sensitive or secret information and intellectual property that an organisation processes. Our recommendation therefore is to have the cyber security controls defined as part of the data security standards and regulations applicable to all organisations that use Internet or cloud technology irrespective of the industry or sector they belong to. For instance, a reference regulation would be the European Cybersecurity Act. Such standards and regulations would cover all data processed by an organisation including personal information. The controls need to be defined based on the sensitivity of the data, the risks to the organisation and to the internal and external customers of the organisation. The Privacy Act should include information on sensitive personal information that needs additional protection. It should define and articulate how this category of data should be shared with other parties. The Privacy Act could refer to the data security standards and regulations under the Australian Privacy Principle (APP) 11 (Security of Personal Information).
Consultation Q9: What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?
We reiterate our recommendation to have cyber security code outside the privacy act and be defined as cyber security controls as part of the data security standards and regulations to expand the scope of its coverage and applicability. However, if it is decided to have enforceable cyber security code under Privacy Act, our recommendation is to consider established standards ISO/IEC (27001, 27701/27018) and NIST Special Publication (SP) 800-53 Rev.5 that have well defined privacy controls. General Data Protection Regulation (GDPR) refers to International Organisation for Standards (ISO) standards when discussing best practices for protection of personal data. Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) refers to NIST standards. Minimum controls that should be enforced through code are: • Encryption of data at rest and in transit • Multifactor authentication for access, access limited only to required data • Maintenance of audit trail of transactions in form of logs • Identification, treatment and continuous monitoring of privacy risks

- Incident management. Reporting high risk incidents to the individuals and to the authorities.

Consultation Q10: What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

All technologies (and composites of technologies), all sectors and all types of information that can uniquely identify an individual on its own or in combination with other data (metadata and/or machine data) should be covered by a code under the Privacy Act. The applicability should be based on the size of the business and type of personal information processed by it. For example, a small local business employing 100 people and processing personal information of its employees related to employment, may be given exemptions from certain obligations under the cyber security code. But a similar sized organisation which has an online business and processes personal information of its consumers or does monitoring of online activities of its consumers or provides surveillance services to other business which involves monitoring and analysis of behaviour of individuals, may have greater obligations under the cyber security code.

Chapter 6 Standards for smart devices

Objective: Defined a mandatory set of baseline standards aligned to those that are already internationally accepted such as NIST CSF, ISO 27001 and ETSI EN 303 645.
Consultation Q11: What is the best approach to strengthening the cyber security of smart devices in Australia? Why?
We suggest that a proportionate approach to be taken is for the Australian Government to provide a set of baseline provisions applicable to all consumer IoT devices that is aligned to those that are already internationally accepted such as NIST CSF, ISO 27001 and ETSI EN 303 645. The Australian Government may also seek to align with the ISA/IEC 62443 series of standards which is structured into the four groups of *General*, *Policies and Procedures*, *System* and *Component* thus providing comprehensive coverage for creation, implementation and usage of Industrial Automation and Control Systems. Additionally, if the Australian Government uses the rubric of the ISA/IEC 62443 series, then IoT Security becomes more a matter of risk management; with each connected device potentially posing a different risk depending upon the threats it is exposed to as well as the likelihood of those threats, the inherent vulnerabilities in the system, and the consequences if the system were to be compromised. This may enable a centrally maintained register of device types with defined threat vectors and risk tolerances to be created and would allow consistent and harmonised design, implementation, assurance and remediation activities to take place.
Consultation Q12: Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for as a standard for smart devices? If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate? If not, what standard should be considered?
YES - We believe that ESTI EN 303 645 be an appropriate international standard for Australia to adopt. However, we would strongly suggest that the full suite of cyber security provisions for consumer IoT be introduced especially 5.8 Ensuring that personal data is secure.
Consultation Q13: [For online marketplaces] Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?
Not Applicable

Consultation Q14: What would the costs of a mandatory standard for smart devices be for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?
We consider that a globally aligned mandatory standard may have an initial cost increase for manufacturers, however this could most likely be capitalised initially and then amortised over the period of the lifetime of the device. However, we also note that in many countries around the world there are tax incentive provisions for Research & Development (R&D) type activities. We would caution that in the event of exceptional additional mandatory standards solely in Australia, the cost would be expected to increase locally on a disproportionate basis.
Consultation Q15: Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?
We consider 'consistency of approach' will ultimately reduce cost to the Australian consumer as well as providing increased consumer confidence.

Chapter 7 Labelling for smart devices

Objective: Established a labelling system equivalent to the UK's 'Kitemark' scheme to provide Australian consumers a clear indicator of an IoT product's or an organisation's level of security and privacy to enable consumer confidence.
Consultation Q16: What is the best approach to encouraging consumers to purchase secure smart devices? Why?
If all the available options presented to consumers are secure by design / implementation devices, it will not be necessary to encourage them as they will be choosing from a pre-existing pool of secure devices.
Consultation Q17: Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?
We believe that an approach equivalent to that recently implemented as part of the reclassification of medical devices (incorporating both software and hardware) as defined by the Therapeutic Goods Act 1989 is practical and sets a ready example of the process that could be followed.
Consultation Q18: Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not? If so, which existing labelling scheme should Australia seek to follow?
While we acknowledge that many industry sectors have codes of practice inter alia for their members that include compliance arrangements these tend to be for inter-profession arrangements. In the interests of the ultimate consumer, we would recommend a mandatory system of labelling for smart devices. Again, we offer that the Therapeutic Goods Administration (TGA) example provides a suitable for template that can be adapted as part of an ongoing Industry-Government-Consumer refinement process.
Consultation Q19: Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?
In our view, a mandatory security expiry date label would be an appropriate step to make in a system akin to the TGA, where safety is to be increased using the Unique Device Identification (UDI) system for medical devices. This allows for tracking and tracing of medical devices including those that have been implanted in patients. This enables accelerated notification and remediation if there is a safety issue identified with a medical device.
Consultation Q20: Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?
We consider that given the increase consumer health related information that is created, stored and transmitted through mobile phones, wearable devices and related applications when combined with the increasing volume of mobile phone related security incidents; it may prove to be a useful addition to include them. However, it may be necessary to phase such inclusion over a period to allow manufacturing organisations to adapt accordingly.

Consultation Q21: Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

We offer that it would be beneficial to label smart devices both digitally and physically.

This is because we agree with the TGA position that states the following benefits to consumers and industry – specifically and in their own words:

"Identification of medical devices using the UDI system will offer significant benefits throughout the supply chain. These include:

- *a reduction in medical and surgical procedural errors by allowing healthcare professionals and others to quickly trace a device and obtain vital information about its characteristics*
- *the ability for patients and consumers to more easily find information relating to devices, through the Australian UDI Database (AusUDID), the Australian Register of Therapeutic Goods (ARTG) and other similar services and databases*
- *improved post-market surveillance due to the ability to identify models of devices on a national and global basis*
- *a more robust and secure global distribution chain*
- *improved ability for data sharing across regulators and the healthcare industry*
- *enhanced research and analysis through the uniform documentation of devices in electronic health records, clinical information systems, registries and other data sources."*

Chapter 8 Responsible disclosure policies

Objective: Established and appropriately empower a body to assess compliance with the mandatory set of baseline standards to provide ongoing assurance to the Australian consumer and to address any areas of non-compliance with measurable action plans. It should assess and validate the remediation of higher risk vulnerabilities that have been identified to reduce potential harm.

Consultation Q22: Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

Responsible disclosure can take three (3) forms which are:

- **Form 1 (incident or breach disclosure):** We already have mandatory breach notification process as part of the Privacy Act and sector-based regulations (e.g. CPS-234 for financial services). This was not the focus of the consultation paper however we believe this is good practice and enforcement should be strengthened to ensure compliance
- **Form 2 (internal vulnerability management):** In this context a high risk / material vulnerability is identified through the normal course of business (e.g. internal vulnerability management program) however cannot be remediated in a timely manner. Sectors like financial services governed by CPS-234 require APRA to be notified within 10-days if a material control weakness (vulnerability) cannot be remediated in a timely manner. We believe a similar notification or disclosure requirements should extend to other sectors for organisations that meet the threshold for the potential impact to society or the economy
- **Form 3 (new vulnerability identification by an external party):** This was the focus of the consultation paper and relates to the identification of vulnerabilities in a **product or service** by a third party. Our response below focuses on this third form of responsible disclosure.

Our recommendation is to make responsible disclosure policy (Form 3) mandatory for organisations that meet the threshold for the potential impact to society or the economy. The impact could be physical, financial or reputational. This policy should be supported by a framework that includes:

- Organisations take a risk-based approach to fix vulnerabilities within a stipulated timeframe (notice period)
- Vulnerabilities which can have a significant impact to society or the economy should be disclosed to the Australian Cyber Security Centre (ACSC) as soon as it is validated (within the notice period)
- Organisations have protection against vulnerabilities being disclosed to unauthorised third parties during the notice period
- Ethical security researchers have protection when complying with the established process to test and report vulnerabilities in good faith (e.g. similar to whistle-blower policies for APRA regulated entities)
- An escalation path is defined for security researchers if organisations do not respond adequately within the notice period. We propose to leverage the ACSC as a potential escalation path with responsibility to compel the organisation to act and/or facilitate public disclosure of the vulnerability

- A policy for recognition of security researchers who have contributed to the identification of new vulnerabilities
- Potential voluntary bug bounty schemes by organisations to encourage independent security research.

The disclosure of incidents and vulnerabilities in all its forms facilitates a healthier ecosystem that ultimately strengthens Australia's cyber security posture. Examples include disclosure of:

- Incidents (Form 1) compel organisations to inform their customers of breach in a timely manner and organisations wanting to protect their reputation have a higher likelihood to provide support services (e.g. credit monitoring for impacted consumers). This data also helps cyber insurance providers to better tailor their policies and premiums to better serve the Australian market as a whole
- High risk vulnerabilities that cannot be remediated in a timely manner to an industry regulator (Form 2) increases visibility to authorised entities who are then able to take proactive action to protect citizens and/or the economy
- Digital product or service vulnerabilities (Form 3) in a timely and secure manner allows Australian organisations to take steps to mitigate the risk before threat actors can exploit them. It also allows organisations to make better risk decisions when evaluating products, services or providers they want to use or engage.

Chapter 9 Health checks for small businesses

Objective: Established a labelling system equivalent to the UK's 'Kitemark' scheme to provide Australian consumers a clear indicator of an IoT product's or an organisation's level of security and privacy to enable consumer confidence.

Consultation Q23: Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?

In general, we support a cyber security health check program to improve Australia's cyber security posture. To throw caution in the wind, health check programs that are based purely on self-assessments can end providing a false sense of security for consumers of the program (e.g. large businesses). We recommend that the program includes some form of validation of self-assessed controls. This can take a form of self-assessments with supporting evidence which is validated by a governing authority. Self-assessment which includes evidence validated independently may strike the right balance however it will increase program costs. We also recommend publishing a centralised register of organisations of who participated and can be used by consuming organisations to perform their due diligence.

Consultation Q24: Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?

Small business would benefit commercially from a health check program if the right incentives are in play. Potential incentives to consider include:

- Corporate tax incentive for organisations who participate and actively demonstrate they have invested to reduce risk
- Federal and state government requirement of a health check to be completed before they can participate in tenders (e.g. like SOC2 certification for large enterprises)
- Publishing a centralised register of participants who have demonstrated good practice for managing cyber risks. The branding and management of this register can foster stability in the ecosystem and improve consumer confidence.

Consultation Q25: If there anything else we should consider in the design of a health check program?

Additional considerations in the design of a health check program for small businesses include:

- Easy to use with relevant online training and support
- Focus on a small set of key controls
- Link to strategic vendors who due to scale can provide cost efficient services for small businesses to remediate issue identified
- Health checks should be time bound with a requirement for annual recertification. The policy can also consider the need for ad-hoc review especially after adverse events (e.g. a breach).

Chapter 10 Clear legal remedies for consumers

Objective: Established and appropriately empower a body to assess compliance with the mandatory set of baseline standards to provide ongoing assurance to the Australian consumer and to address any areas of non-compliance with measurable action plans. It should assess and validate the remediation of higher risk vulnerabilities that have been identified to reduce potential harm.
Consultation Q26: What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?
As called out in the consultation paper, there has been limited recourse for consumers of digital products and services (especially if the vendor is based overseas). There has also been limited coverage of potential precedence for such actions taken in the past. As a result, the priority should be clarification of the definition of digital products and services and obligations by vendors. It would also be good if similar laws exist with our major trading partners therefore ensuring that Australian consumers may have legal recourse although the vendor is based overseas.
Consultation Q27: Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?
The reforms being considered, such as the below would significantly benefit individuals: • Direct right of action under Australian Consumer Law and Privacy Act 1988 • Penalties for breaches that have significant impact on individual's privacy leading to loss, financial or otherwise, or harm to the individual. Other actions that Government could consider related to processing of certain categories of personal information outside boundaries of Australia are: • Enforcing organisations to provide additional protection to the Sensitive information like the health and financial information being processed outside the boundaries of Australia or putting restrictions to processing of such data outside Australian boundaries • When Australian citizens' data is collected within Australian boundaries and is being processed outside the country, the citizens should enjoy similar level of privileges, be able to exercise their rights and take legal recourse in case of breaches, like the privileges they enjoy in the country • Processing outside boundaries of Australia should only be with consent of individuals whose data is being processed. Some examples to quote from other geographies are: • The Schrems II decision has brought amendments to GDPR on processing of personal data outside EU

- The Government of Canada restricts certain category of government data being processed outside Canadian boundaries. Similar restrictions on public sector data and government data are imposed by privacy laws of provinces such as Quebec, Nova Scotia and British Columbia.

Chapter 11 Other issues

Objective: Defined a mandatory set of baseline standards aligned to those that are already internationally accepted such as NIST CSF, ISO 27001 and ETSI EN 303 645.
Consultation Q28: What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights of consumers?

- Cyber security regulations pertaining to the manufacture and usage of emerging technologies like IoT and drones are required to protect society's privacy and security. For example, the UK is coming up with legislation to control smart devices including IoT devices. US has enacted the Internet of Things Cybersecurity Improvement Act of 2020 (the “IoT Act”) that mandates cybersecurity standards and guidelines for the acquisition and use of IoT devices by the federal government. California and Oregon have enacted IoT laws covering all connected devices and specifying reasonable security features that manufactures of connected devices must adhere to.

- Another area where the organisations could benefit from each other's experience and help build stronger cyber security is by sharing threat data within sectors and across industries. There are already Information Sharing and Analysis Centres (ISACs) across various sectors however the speed at which intelligence is shared needs to improve. The Kaseya supply chain attack earlier in the year is a good example of the speed at which threat actors can exploit vulnerabilities across multiple organisations[3]. New forms collaboration, automation and deep integration is required to share actionable intelligence in a timely manner.

[3] https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

Contributors

Justin Parr-Davies

Partner – APMEA Head of OT & IoT Security Practice

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 the Chief Information Security Officer for a Victorian Statutory Authority as well as the Global Head of Technology Governance, Risk and Assurance at a Global Energy and Resources organisation.

His broad experience in the fields of Cyber Strategy, Governance, Compliance, Risk Management and Assurance for IT, OT and IoT underpins his ability to provide practical advice to his clients on safety assurance matters and the developing domain of Enterprise IT and Operational Technology security convergence.

Justin can be contacted at [redacted]

Ganesha Rajanaidu

Partner – APJ Head of Cyber Consulting

Ganesha has more than 17 years of cyber consulting experience across industry sectors and in the Asia Pacific region. He has previously served as the Asia Pacific Chief Information Security Officer (CISO) for a multinational Australian pharmaceutical organisation and held leadership roles at EY Australia and PwC Australia.

His expertise in strategy, risk management and incident response help clients to develop cyber resilient strategies that drive business outcomes and manage cyber risks to within their appetite.

Ganesha can be contacted at [redacted]

Vrinda Muzumdar

Lead Consultant – Cyber Security and Risk Practice

Vrinda Muzumdar has 25+ years of experience in IT industry, primarily in the area of application program management. For last 6 years she has been involved in Cyber Security and Data Privacy consultancy. She has worked extensively in this domain and has helped clients in Banking, Fintech, Retail and ITES industries to develop and implement privacy programs.

Her experience and expertise in setting up privacy organization, executing privacy programs for large enterprises with cross geography presence and bringing in automation in privacy management with help of privacy tools, helps clients to implement and manage forward looking privacy programs in the evolving world of data privacy.

Vrinda can be contacted at [redacted]

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**