“Enhanced cyber security posture”

WHAT DOES IT REALLY MEAN?

In response to the Ukraine conflict the Australian Department of Home Affairs and the Australian Cyber Security Centre are strongly recommending:

- Organisations in Australia urgently adopt an **enhanced cyber security posture**;
- Companies **voluntarily implement** the obligations proposed in the draft Security of Critical Infrastructure Legislation Amendment, currently before Parliament; and
- Organisations "should urgently work to **identify and resolve risks** that may affect the availability, integrity, reliability and confidentiality of their asset”.*

This poses **three critical issues** for organisations:

1. How do you adopt an “enhanced cyber security posture”?
2. Should you voluntarily comply with pending regulations?
3. Are you prepared to respond to, and accelerate recovery from, high impact cyber incidents?

* See CISC Action Alert here

Cyber action alerts

IMPLEMENTING THE LATEST ADVICE FROM HOME AFFAIRS

1 HOW DO YOU ADOPT "ENHANCED CYBER SECURITY POSTURE"?

The Australian Cyber Security Centre's (ACSC) most recent alert* points to an **increasing threat of deployment of destructive malware**, triggered by events in Ukraine.

While many organisations can implement enhanced measures some are **now overwhelmed with the scale of unactionable threat intelligence** and third party **information requests**.

To adopt an "enhanced cyber security posture" you should consider:

- **Triaging and assessing** threat intelligence so that it is **actionable and meaningful**.
- Implementing additional measures to **boost monitoring, detection and cyber defences**.
- **Revisiting and validating risk-based decisions** and determining if your **risk tolerance still holds** in a threat environment that is likely to be sustained for longer.
- Giving clear and **updated advice and training to all employees** – they are your first line of defence.
- Urgently reviewing your **risk exposure to third parties** (for business continuity and for third parties who may not have active cyber defence capabilities).

2 DO YOU VOLUNTARILY COMPLY WITH PENDING REGULATIONS?

Organisations are now being asked to voluntarily comply with *proposed amendments* currently before Parliament to introduce a requirement to implement a risk management program and enhanced risk measures for systems of national significance.

Voluntary compliance, in the absence of completed industry consultation, puts organisations in a challenging position as the regulatory and industry guidance to ensure compliance is incomplete; yet the ask for you to implement is urgent.

At a minimum you should:

- **Migrate from a compliance and maturity** based form of cyber assessment to a **risk-based assessment**.
- **Re-assess material risk** and identify how **threat actors in the current environment** can impact your business.
- **Understand controls** (physical and technical) and re-assess your critical vulnerabilities.
- Assess your **third party risk exposure** and their role in defending your organisation.
- Be prepared to **respond to customers and partners** who need to understand your risk profile, as part of **their own re-assessment.**

3 ARE YOU PREPARED TO RESPOND AND ACCELERATE RECOVERY?

Even organisations who are confident about their cyber controls **will need to review their preparedness for cyber incidents**.

Consider the following:

- Have you **implemented lessons learnt** from your last cyber simulation exercise? Did your last cyber exercise include **worst case scenarios**?
- Have you **trained delegates** to the same standard as primary members of your incident and crisis response teams?
- Are your **third party security service providers on high alert** and have you clearly articulated **expectations, actions and levels of authority** in the event they detect a significant breach?
- Have **you re-visited your disaster recovery planning** and is it realistic?
- Have you **tested your response and decision governance** (at Board level) in relation to **ransomware demands**? Do you have a **clear legal position** on whether you can pay?
- Do you understand the operational constraints of ransomware payments and have you considered the potential reputational and ethical, as well as regulatory and legal issues?
- Do you have the **appropriate resources and advisors on call** and know how and when you would **notify regulators and authorities**?

* See "ACSC - 2022-02: Australian organisations should urgently adopt an enhanced cyber security posture" here

ashurst

Our cyber expertise

APPLYING AN INTEGRATED LEGAL AND RISK APPROACH

Ashurst's combined Legal and Risk Advisory expertise in cyber security is accessed by large listed companies, global organisations, leadership teams and Boards so they can improve the governance, compliance, risk management and crisis response to cyber security. We have deep expertise in issues such as ransomware, data breaches, geo-politically motivated attacks, regulatory investigations and industry-wide preparedness.

Our recent experience includes supporting clients throughout data breach and ransomware incidents, including advising on crisis management operations, engagement with Threat Actors, the legal and operational issues with ransomware payments, forensic investigations, regulatory notifications, governance and assurance of cyber response and recovery, cyber insurance and managing third party advisors and service providers. We also regularly advise Boards and leadership teams on cyber reporting and metrics, cyber governance, team structure and operating models and cyber due diligence for acquisitions.

CYBER FOR LEADERSHIP

- Boards (Governance and Readiness)
- Executives (Strategy and Readiness)

CYBER RESPONSE

- Ransomware
- Crisis Management
- Incident Management
- High Impact Events

CYBER AS A SERVICE

- CISO selection
- Cybersecurity Programme Management
- Interim CISO
- Retainer arrangements

CYBER COMPLIANCE

- Critical Infrastructure
- CPS 234
- ISO 27000
- Due Diligence
- International standards

OUR TEAM

Sid Maharaj
Partner

Strategic and Cyber Risk
+61 406 568 171
sid.maharaj@ashurst.com

John Macpherson
Director

Strategic and Cyber Risk
+61 2 9258 6479
john.macpherson@ashurst.com

Rob Hanley
Partner

Legal Governance Advisory
+61 436 402 922
robert.hanley@ashurst.com

Andrew Craig
Partner

Digital Economy Transactions
+61 3 9679 3592
andrew.craig@ashurst.com

ashurst