SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE PROTECTION) BILL 2022

CREST welcomes the second Bill to amend the *Security of Critical Infrastructure Act 2018* which captures the remaining elements from the SLACI Bill 2020 along with amendments captured from the review process with stakeholders. CREST is pleased to see the consultancy process working together with amendments suggested by stakeholders.

Enhanced Cyber Security Obligations for Systems of National Significance

CREST and its Member companies in Australia support the amendment to add additional security measures to a small subset of the critical infrastructure that are of particular national significance.

Information sharing

The amendment specifically mentions the importance of enhanced threat sharing and CREST would welcome the opportunity to speak to the Government about how we can help.

The CREST Threat Intelligence (CTI) Professional's Group, CREST's focus group on Threat Intelligence, which is made up of leading threat intelligence providers from around the world to ensure our members and the governments and regulators we work with are kept at the forefront of the CTI industry developments.

It is encouraging to see the Australian Government recognise the importance of intelligence sharing which has been consistently supported by stakeholders. CREST and its Members believe that cyber reliance requires the bi-directional sharing of threat information. Without it we can not hope to protect critical assets from a significant attack.

CREST would be keen to share with government the lessons learnt from the United Kingdom in implementing cyber threat intelligence processes for the protection of critical infrastructure.

Cyber security exercises

CREST has experience in the creation and delivery via its members of bespoke security exercises for specific vertical markets.

For example. CREST's STAR framework delivers controlled, bespoke, intelligence-led cyber security red teaming engagements. STAR incorporates penetration testing and threat intelligence services to accurately replicate threats to critical assets. Since it was first delivered STAR has been adapted and used as a baseline for many other industry schemes, including ones that focus on Financial Services, Telecommunications and Critical National Infrastructure.

A good example of this is CBEST - developed along with the UK central Bank, the Bank of England, to deliver controlled, bespoke, intelligence-led cyber security tests that replicate behaviours of those threat actors, assessed by Government and commercial intelligence providers as posing a genuine threat to systemically important financial institutions. CBEST was the first initiative of its type to be led by any of the world's central banks.

BENEFITS:

- access to advanced and detailed cyber threat intelligence.
- access to knowledgeable, skilled, and competent cyber threat intelligence analysts who have a detailed understanding of the financial services sector.
- realistic penetration tests that replicate sophisticated, current attacks based on current and targeted cyber threat intelligence.
- access to highly qualified penetration testers that understand how to conduct technically difficult testing activities whilst ensuring that no damage or risk is caused.
- confidence in the methodologies utilised by the companies within CBEST for conducting these sophisticated and sensitive tests.
- confidence that the results and the information accessed by the testers will protected.
- standard key performance indicators that can be used to assess the maturity of the organisation's ability to detect and respond to cyber-attacks.
- access to benchmark information, through the key performance indicators, that can be utilised to assess other parts of the financial services industry.
- a framework that is underpinned by comprehensive, enforceable, and meaningful codes of conduct administered by a specialist professional body.

This scheme can be readily tailored for any critical infrastructure sector within the Australian market and delivered by Australian based CREST member companies. This would provide the Australian government with a baseline of assurance against cyber resilience of organisations within the critical infrastructure regime.

External auditor

The document mentions use of an external auditor if the Secretary has reasonable grounds to believe that an evaluation report was not prepared appropriately. However, there's no requirement specified for that external auditor to meet specific standards - as say an engineer or accountant might. Whilst the external auditor is a specified individual authorised by the Secretary, CREST would argue this person should meet a high threshold of technical ability, acknowledged by being the holder of a CREST Certified exam. This level of ability would provide assurance to the market then external auditor is technically competent as measured against an international skillset.

Incident response

While of course preventing attack is essential it is also crucial to improve incident response, particularly for critical assets. Along with vulnerability assessment, penetration testing, threat intelligence and SOC, CREST also accredits incident response providers. In the UK the Centre for the Protection of the National Infrastructure has formally endorsed the CREST Cyber Security Incident Response (CSIR) scheme.

This scheme can easily be exported to Australia and tailored to local requirements. It would also provide a level of assurance for those owner/operators of critical infrastructure that operate in international markets.

Designated officers

With regards to the mention of designated officers (likely AG/ASD) to conduct the vulnerability assessment activities, CREST would welcome the opportunity to discuss with the Commonwealth regarding the feasibility of opening this activity to be delegated to suitability a qualified and accredited organisation. This could include those who have signed up to CREST's strong Code of Conduct and Code of Ethics to become an accredited vulnerability assessment services provider.

About CREST - www.crest-approved.org

CREST is a not-for-profit accreditation and certification body representing the technical information security industry. CREST provides internationally recognised accreditations for organisations providing technical security services and professional level certifications for individuals providing vulnerability assessment, penetration testing, cyber incident response, threat intelligence and security operations centre (SOC) services. CREST Member companies undergo regular and stringent assessment, whilst CREST certified individuals undertake rigorous examinations to demonstrate the highest levels of knowledge, skill and competence. To ensure currency of knowledge in fast changing technical security environments the certification process is repeated every three years.

CREST is governed by an elected Executive of experienced security professionals who also promote and develop awareness, ethics and standards within the cyber security industry. CREST supports its members and the wider information security industry by creating collaborative research material. This provides a strong voice for the industry, opportunities to share knowledge and delivers good practice guidance to the wider community.

CREST has 300 Members internationally with 55 Members in the Australian market.

CREST welcomes the opportunity to work with the Australian Government on these initiatives to create a stronger, more prosperous critical infrastructure sector. To arrange a conversation please contact Nigel Phair, Chair of CREST in Australia email [redacted] /
[redacted]