Harmonisation of cybersecurity risk management legislation, regulation, frameworks and standards

Supporting national security, corporate security, economic security and international trade

I. Affects of cyber.
II. Cybersecurity risk management regulations.
III. Effects of cybersecurity risk regulations.
IV. Conclusion

ONCD National cyber strategy (March 2023): '*The Strategy recognizes that government must use all tools of national power in a coordinated manner to protect our national security, public safety, and economic prosperity*.'

The Augusta Group

I. Effects of cyber

Cyberattacks pose a significant threat to national security

- Cybersecurity is a complex and expensive risk to manage. Attacks originate from nation states, nation state backed actors, criminal gangs, script kiddies, hacktivists, terrorists and all of the above combined.
- Cyber attacks and cybersecurity poses a significant direct and indirect risk to national security, corporate security and economic security[1,2].
- National security is dependent upon corporate cybersecurity. Corporate cybersecurity is dependent upon national security – CNI providers are invariably commercial organisations.
- Market forces alone have failed to address the needs of cybersecurity. Cybersecurity is an commercial consideration for the private sector[3].

The affects of cyber attacks and a poor cyber posture affect national, corporate and economic security. Driving cybersecurity risk management regulation.

II. Cybersecurity risk management regulations (1)

U.S and EU Cyber Legislation, and Regulation (illustrative, incomplete)

Several nation states and industry regulators have taken significant steps to regulate cybersecurity.

U.S – Federal Government

- Federal Information Security Modernisation Act (FISMA) – 2002, 2014, 2022[4].
- DFARS 252.204-7012 – Applied to U.S DoD supplier contracts from 2017[5].
- White House National Cyber Strategy – March 2023[1].
- Securities and Exchange Commission (2022) – Cybersecurity risk management (Proposed rule)[6].
- Food and Drug Administration(FDA) - Cybersecurity regulations for medical devices (October 2023)[7].

Cybersecurity risk management regulations (2)

U.S and EU Cyber Legislation, Regulation and Enforcement Regimes

European Union

- Network and Information Security Directive 2.0 (EU NIS 2.0 - 2023)[8].
- Digital Operational Resilience Act (DORA – 2023)[9].
- Cybersecurity Resilience Act (2022 - Provisional)[10].
- Cybersecurity Solidarity Act (2023 – Provisional)[11].

The adoption of cyber regulation and enforcement regimes by national states and industry regulators aim to address national security corporate security and economic security.

III. Affects of cybersecurity risk regulations

Harmonisation and standardisation of cybersecurity risk management

Cybersecurity regulation affects national security, corporate security and economic security. Affecting trade in and with those countries that are moving ahead with regulation.

- Regulatory compliance affects access to markets.[5,6,7,8,9,10]
- National and industry regulators are setting the bar for compliance and evaluated through regulatory oversight of frameworks and standards.
- Cybersecurity regulatory compliance creates differentiation. As compliance to higher standards attracts trade, investment and facilitates insurance.
- Regulatory compliance drives significant and varying costs of compliance, between jurisdictions and industry sectors.
- Cyber regulation affects corporate legal and compliance risk.

Cybersecurity is a NATO domain of operation. Cyber regulation is required to improve national security, corporate security and economic security. While setting the bar for cybersecurity compliance.

IV. Conclusion

Harmonisation and standardisation of cybersecurity risk management

- National security and the success of the digital economy relies upon cybersecurity. Cybersecurity that is being regulated by nation states and industry regulators.
- Global trade is facilitated through global and local ICT products and services. Products and services that will be affected by cybersecurity regulation.[8,9,10]
- Cybersecurity regulators are defining the minimum standards for cybersecurity and risk management compliance. Minimum standards that national agencies and organisations will be required to achieve, in some cases for market entry.

Opportunity

- Collaboration on cybersecurity risk management regulation will achieve a successful outcome for national, corporate and economic security.
- The harmonisation and standardisation of cybersecurity and risk management regulation will facilitate common and agreed cybersecurity frameworks and standards.
- Harmonised and standardised cybersecurity frameworks and standards will facilitate regulatory compliance and reduce the cost of compliance.

Cybersecurity risk management regulation is developing rapidly. Is now the time to start a dialog on the harmonisation of cyber regulations, frameworks and standards?

Cybersecurity risk management regulations

U.S and EU Cyber Legislation, Regulation and Enforcement Regimes

Note:

1. https://www.whitehouse.gov/oncd/#:~:text=ONCD%20coordinates%20a%20whole%2Dof,innovation%20through%20cybersecurity%20policy%20leadership
2. https://www.linkedin.com/feed/update/urn:li:activity:7052482187207577600/
3. https://www.csis.org/analysis/conversation-chris-inglis-and-anne-neuberger-0
4. https://www.congress.gov/bill/113th-congress/senate-bill/2521
5. https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
6. https://www.sec.gov/news/press-release/2023-52
7. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-refuse-accept-policy-cyber-devices-and-related-systems-under-section
8. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN
9. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554&from=EN
10. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act
11. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity#:~:text=The%20EU%20Cyber%20Solidarity%20Act%20aims%20to%20strengthen%20capacities%20in,scale%20cybersecurity%20threats%20and%20attacks.