THE AUGUSTA GROUP

U.S and EU cybersecurity regulations enforce cybersecurity risk management '*Left of Bang*' and into the financial statements of covered entities

Cybersecurity is a compliance problem for boards to resolve

By: Andy Watkin-Child & Ted Dziekanowski

February 2023

Introduction - Left of Bang.

In '*Left of Bang, How the Marine Corps' Combat Hunter Program can save your life'* by Patrick Van Horne and Jason A. Riley[1], the importance of situational awareness in combat is discussed and the situational awareness that cyber regulation will enforce into the board room of covered public and private sector organisations. The concept of '*Left of Bang*' is simple, it is to raise situational awareness, provide early warnings and prevent attacks from taking place by enabling those that are potential targets, identify the pre-event indicators and warning signs of an attack and to be proactive in managing threats, vulnerabilities and associated risks, rather than reactively managing incidents. That is in essence the requirements for effectively managing cybersecurity risk.

Traditionally organisations have been more reactive to the management of cybersecurity risk, adopting a stance of '*that won't happen to me*' and ignoring the risk or relying on the purchase of cyber insurance to treat the risk by transferring the risk through the insurance policy. However, the rise in successful cyber-attacks in 2021 and 2022 has challenged cyber insurers and their customers to find a cost-effective means of continuing to provide a risk transfer mechanism while remaining economically viable.

Governments, recognising the peril to critical infrastructure have begun to swing away from market forces being a determinant for the management of cybersecurity, and instead are adopting a regulatory approach to cybersecurity where the focus is heavily placed on the management of cyber risk. Such regulation includes the Securities and Exchange Commission's (SEC) cybersecurity risk management, strategy, governance, and incident disclosure proposal[2,] and the US Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC)[3] regime, focusing on the global Defense Industry Base (DIB), under Defense Federal Acquisition Regulatory Supplements (DFARS 252.204-7012)[4]. Similarly, the EU has released the Network and Infrastructure Security 2.0 (EU NIS 2.0)[5] Directive and the Digital Operational Resilience Act (DORA)[6] affecting the suppliers of Critical National Infrastructure and Financial Institutions (both now on the EU Journal). In 2022 both US and EU regulators proposed that manufacturers of ICT products and services certify to cybersecurity risk management standards before products and services can be sold in the U.S[7] or EU[8].

Q1 2023 should see the release of the White House Office of the National Cyber Director (ONCD) National Cybersecurity Strategy, reaffirming Chris Inglis' statement that cyber regulation is required to manage cyber risk. The SEC is expected to release its cybersecurity risk management regulation in H1 2023, affecting firms that require access to US capital markets. The DoD CMMC programme roll-out timeline is unclear but DFARS 252.204-7012 and requirements for defence contractors to comply with NIST 800-171 are in place and enforceable. EU Member States have 21 months to convert EU NIS 2.0 and DORA into their National Laws and it is expected that the EU will release a proposed Cyber Resilience Act (CRA) in 2023.

The impact of US and EU cybersecurity regulation on the boardroom

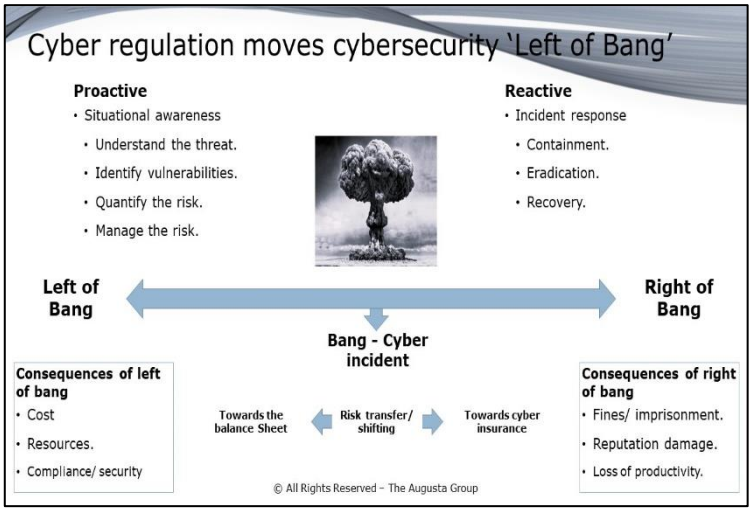
The results of current, pending and proposed cyber regulations will be to drive cybersecurity risk management compliance into the board rooms of covered entities. Boards should anticipate being required to implement a cybersecurity risk management strategy, governance, a cybersecurity risk management framework, a cybersecurity program, risk management and cyber standards, board oversight, assurance and attestation of cybersecurity risks, incident, and regulatory reporting.

In response to these regulatory, financial, and legal challenges, boards will be required to demonstrate their organisations' 'situational awareness' of cybersecurity through cyber risk management. Boards will have to document, attest, and report their personal experience and knowledge of cybersecurity risk management, the management of their organisations cybersecurity risks and those that extend across their supply chains. They will have to demonstrate governance over the management of the threats, vulnerabilities, and associated cybersecurity risks to their corporate financial statements.

The aforementioned will be enforced by regulators. That could result in outcomes ranging from corporate and personal regulatory fines, increased cost of capital through rating agency downgrades, lawsuits from dissatisfied shareholders and activist board members seeking to influence the direction of the organisation and the decisions of their board members.

Cybersecurity regulation transfers cyber '*Left of Bang*', into the board room and to the organisation's financial statements.

Cyber regulation reduces the choices covered organisations have for managing cybersecurity. The widely recognised '*it won't happen to me*' approach to cybersecurity', managing a cyber incident '*Right of Bang*'' and relying on cyber insurance to manage the cost of a cyber-attack, are becoming unrealistic options in today's economic environment. Regulation will define the '*choices*' available to covered entities for cybersecurity compliance. Covered entities can choose to manage cybersecurity risk, attempt to leave the regulated market, or accept the risk of sanctions if they fail to comply. A consequence of failing to comply may make a successful insurance claim more difficult as a cyber incident may raise questions over an organisation's compliance with cyber regulations. Failing to comply with cyber regulation could be used as the basis for refusing to pay out against a policy. The absence of the full transfer of cyber risk to an insurance company and the



requirement to comply with cyber regulation shifts the cost of managing cyber risk onto the financial statement of covered entities.

Cybersecurity risk management regulation places the onus on boards to manage cybersecurity risks and related controls (which are largely preventative) '*Left of Bang*'. Cyber regulation requires organisations to proactively develop the situational awareness that enables them to manage cybersecurity risks, better react to the changing cyber threat landscape and report cybersecurity risk management compliance to regulators. For example, the SEC proposal requires organisations to disclose their cybersecurity risk management strategy and governance, policies and procedures, cyber program and updates to cybersecurity risk management if an organisations business strategy, financial outlook, or financial planning change. The covered organisation will have to declare the board members knowledge and experience in cybersecurity and inform the SEC of a cyber incident within 4 business days. All of which requires an understanding of an organisation's situational awareness as it relates to cybersecurity risk management.

How '*Left of bang*' can deliver cyber compliance into the board room

Cyber regulations such as EU NIS 2, DORA and the SEC proposal require boards to manage cyber risk. That raises the question '*can an organisation rely on cyber insurance as the sole risk treatment?*' given market conditions that make cyber insurance expensive, with reduced coverage and exclusion clauses focusing on nation state threat actors. The introduction of additional cyber regulation complicates the governance challenges boards face, where a lack of knowledge and/ or experience can lead to costly errors hampering the effective allocation of capital.

Cyber regulatory compliance requires organisations to provide additional funding to manage cybersecurity risks. Costs that may include the evaluation of cybersecurity risk, the implementation of cybersecurity programs, governance, oversight, assurance, and attestation. In addition, regulators have been clear that boards must understand the impact of cybersecurity across their supply chains and be assured that third parties have a balance sheet capable of absorbing potential losses that result from a cyber incident that affects their customers.

Cyber regulations increase boards' legal and compliance risk and that of their executive officers and security professionals (CISO). Boards will be required to attest to cybersecurity risk management, report their knowledge and experience and disclose cyber incidents following oversights from risk, audit, cyber, legal and compliance committees. This will necessitate the adoption of a three Line of Defence (3 LoD) model similar to that adopted by covered financial institutions under Basel accords. Cybersecurity risk management compliance is a double-edged sword. Failing to comply creates legal and compliance risk while compliance necessitates situational awareness, cybersecurity risk management and open and transparent disclosure.

An example of the legal risks that cyber regulations create include the recent Uber CSO and Drizzly cases. These actions demonstrate an approach regulators appear to be taking in respect to an organisation's handling of cyber incident management and reporting. This approach will evolve as regulators expect boards and security professionals to have greater accountability and responsibility for cybersecurity risk management.

How do boards address cybersecurity risk management compliance?

The onus that cybersecurity risk management regulatory compliance places on boards necessitates a '*book of work'* that involves stakeholders from inside and outside of the organisation. A book of work must be owned by a member of the board, who has the responsibility and accountability to oversight and assure risk. That could be the Chief Risk Officer, Chief Audit Officer, Chief Compliance Officer, or General Counsel. This is not a project that is run by the CIO or CISO, as they are usually the executives responsible for the cybersecurity program. They do not own enterprise-wide risk and are arguably accountable and responsible for implementing the solutions to mitigate cyber and technology risk.

The 3 LoD model sets out a structure that identifies those that create and manage risk (1st Line), those that assure risk (2nd Line) and those that provide independent oversight of risk (3rd Line). Cybersecurity risk management compliance should be owned by an independent director governed by the board and taking feeds from the various board reporting committees to take an objective view of compliance. As compliance is a regulatory and legal requirement the best placed board member to oversee a book of work in the first instance is likely the Chief Risk Officer, Chief Compliance Officer (2nd Line) or General Counsel.

Now is the time to prepare for cybersecurity risk management regulation. If your organisation is a covered entity that trades in, or with, the U.S or EU, we recommend the following steps.

Step 1: Acceptance and Impact Assessment – Cybersecurity is a strategic, regulated and complex '*Left of Bang*' risk for boards to manage. Boards need to:

1a. Accept that cybersecurity risk management is moving '*Left of bang*'. It is a regulatory, compliance and legal risk that boards must face if they are a covered entity. It is a risk that sets out clear obligations for boards to govern cybersecurity risks, oversight, and assurance of cybersecurity compliance.

1b. Be clear that cybersecurity is a strategic enterprise-wide business, not a technology risk. All functions and departments across the organisation have a role to play in cybersecurity risk management.

1c. Accept that cybersecurity risk management is integral to all business decisions. e.g.. the SEC cyber proposal expects organisations to re-evaluate cybersecurity risks with changes in business and operational strategy and financial performance.

1d. Be clear about the security over the organisations 'crown jewels' and the impact this would have to the organisation should they be damaged, lost or stolen and the remedial actions to maintain resilience.

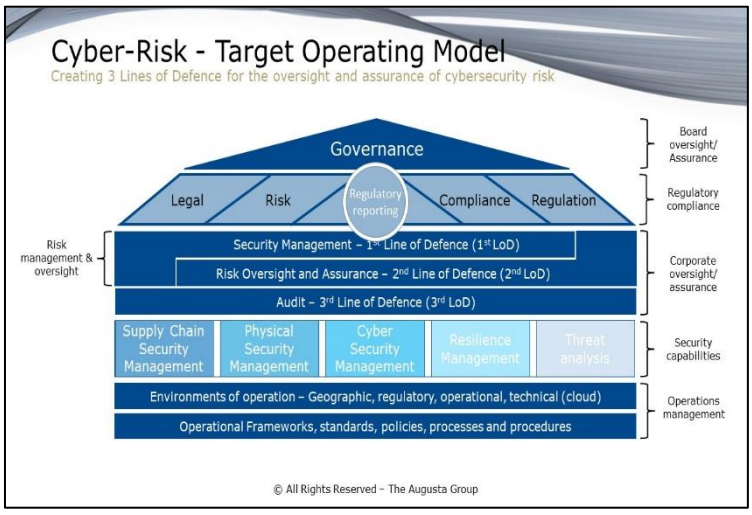
1e. Have a clear understanding of regulatory and legal commitments across the jurisdictions in which the organisation operates.

Boards should be clear about their legal commitments and the necessary plans of action to mitigate cyber risks. Regulators such as the U.S Department of Justice (DoJ) are keen to ensure cyber regulatory compliance and are actively developing regulatory compliance programs.

Step 2: Governance – Board oversight, assurance and attestation of cyber risk requires boards to implement a governance framework.

Regulators expect boards to take an active role in the evaluation, oversight, assurance and management of cybersecurity risks which includes declaring the organisations cybersecurity governance and the knowledge and experience the board of directors has over the management of cybersecurity risks (e.g., the SEC Proposal). Cybersecurity risks are complex and cross many areas of organisational expertise. It is important therefore that boards implement the appropriate governance structures to enable cyber risks to be evaluated by competent and qualified professionals. Evaluations are driven up through the organisation's governance structures to the board for appropriate oversight, assurance, attestation and reporting enabling boards to provide a reasonable level of assurance that inherent risk, control effectiveness and residual risks are managed.

Step 3: Target Operating Model (TOM) – An effective approach to demonstrating cybersecurity risk management governance and compliance is using a Target Operating Model. A TOM provides a structure that aligns key stakeholders, deliverables, policies, processes, and procedures and clarifies roles and responsibilities of risk ownership, evaluation, mitigation and reporting.



An organisations internal and external stakeholders should include legal, compliance, regulatory, risk, audit, front, middle and back-office functions and suppliers who are accountable and responsible for the creation, management, oversight, assurance and reporting of cybersecurity risks. Risks that the audit, risk, IT, cyber, human resources, strategy, and operations committees coordinate, oversight, assure and report to the board executive committee.

A TOM provides a structured approach to govern risk. It describes the organisation's structure, departmental and functional roles and defines the responsibilities and accountabilities of key stakeholders for the management of cybersecurity risks. These roles, responsibilities and accountabilities are formalised through policies and procedures that can be managed and evaluated by 1st, 2nd and 3rd Lines of Defence to oversight and assure compliance.

Step 4: Compliance. *Cybersecurity risk management* and *cybersecurity* are closely related but they are not the same. Cybersecurity has often been achieved by compliance with international cybersecurity standards such as ISO 27001, NIST SP 800-53, NIST SP 800-171, Cloud Security Alliance (CSA) or Centre for Internet Security (CIS) controls. These standards set out important cybersecurity principles, practices and control objectives that organisations aim to achieve to manage cybersecurity, but more often they do not set out the standards by which cybersecurity risks are to be identified, qualified, quantified, remediated, and reported which is required by cybersecurity risk management regulation.

Cybersecurity risk management compliance is structured by the TOM and delivered through the cybersecurity risk management compliance program. The program develops and implements the appropriate TOM, the cybersecurity risk framework, cybersecurity standards, policies, processes and procedures required to deliver cybersecurity risk management. It provides oversight of cybersecurity risk assessments, control effectiveness, the Plans of Actions and Milestones (POAM) required by the organisation's stakeholders to demonstrate cyber risk mitigation and coordinates the oversight and assurance required by the organisation's committees and board.

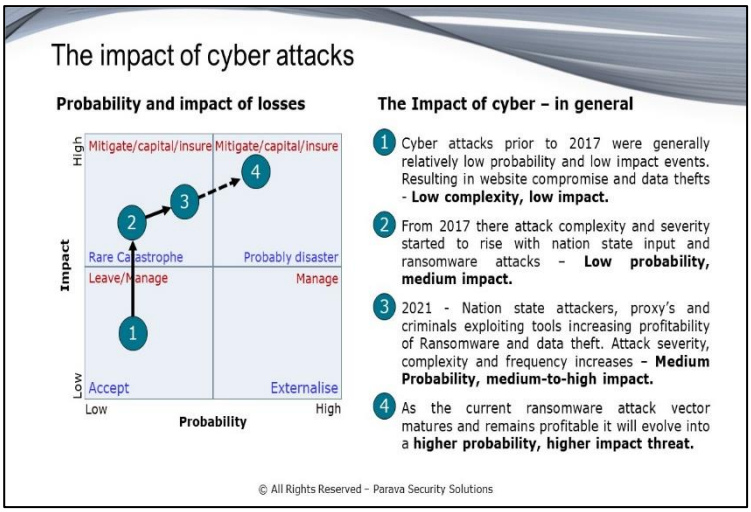
Step 5: Oversight, assurance, and reporting – Board members are required to take an active role in the oversight and assurance of cybersecurity and risk management. Boards need to seek expert advice from sub-committees that provide oversight and assurance across their field of professional expertise, such as cybersecurity, risk, audit, legal, compliance, operations, Human Resources, IT and digital.

The penalties that organisations and boards face for cybersecurity risk management compliance warrants a formalized approach to oversight and assurance cybersecurity compliance, requiring clearly defined board reporting, following a broad range of inputs from across the organisation. Appropriate and agreed Key Performance and Risk Indicators (KPI/ KRI) are fed into board sub committees such as the audit, risk, cybersecurity, IT, compliance, third party supplier and operations for evaluation. Strategy, finance, operations and cyber risk management is assessed, POAMS agreed and the effects of risk mitigation is evaluated. Outputs from these committees are fed to the board committee for final evaluation, approval and attestation prior to the submission of an agreed regulatory response.

It is important the boards demonstrate that they have appropriate governance in place to oversight and assure cybersecurity. Seeking advice and guidance from internal and external expertise, that includes cybersecurity experts, third party audit and legal is important.

Conclusion

Cyber regulation requires boards to evaluate their treatment of cybersecurity risk. The traditional approach for many has been to rely on cyber insurance as the main form of risk transfer. Cybersecurity is simply too expensive a risk to manage and for the 99% of organisations that are SMEs/ SMBs, cyber insurance is the only tool that many organisations have to manage cyber. The absence of cyber regulation has allowed boards to 'choose' to manage the risk; a choice that has been rightly based upon the economics of deploying cybersecurity and the perceived return.



This was based on cyber being a low probability low impact event. This is no longer the case and cyber is a risk that should be treated as a likely and high impact event. It is a risk whose impact is considered by U.S Government, Federal agencies and the EU commission to be high enough that it warrants regulation in response to the concerns that cyber presents to the public and private secto, and the insurance industry that has found cyber a difficult risk to manage. Ransomware as the predominant threat vector is not expected to reduce in severity of impact until organisations take steps to manage the risk.

Cybersecurity has a cost of compliance both 'left and right of bang'. 'Right of bang' costs are generally associated with incident response and remediation, brand and reputational damage, regulatory compliance and legal expenses and lawsuits. These are costs many organisations either self-fund or rely upon cyber insurance to cover. '*Left of bang*' costs are associated with implementing cybersecurity and the frameworks, standards, and practices for managing cybersecurity risks and controls. Traditionally organisations have found '*Left of bang*' costs too high, relying on 'it won't happen to me' and cyber insurance to cover cyber incident costs, rather than implementing cybersecurity risk management.

Cyber regulation however transfers cybersecurity risk management '*left of bang*', increasing the costs of compliance through the application of risk management and effective preventative controls. The SEC cybersecurity proposal, EU NIS2 and DORA set expectations that boards manage cybersecurity risks, attest to their cyber knowledge and experience and report cyber risk compliance to regulators. Cybersecurity regulation forces boards to accept that they have to manage cyber risk (if they wish to stay in a given market), accept the capital allocation for cybersecurity onto the balance sheet that is to the detriment of the organisation's capital allocation. Cyber regulation requires boards to evaluate cyber risks below their historic levels of risk appetite and manage cybersecurity appropriately. Regulation removes the ability of the board to make decisions based upon the cost of implementation alone. It requires boards to demonstrate a reasonable level of cyber compliance, that while economic in nature

has to be justified in line with the boards responsibility to demonstrate due diligence and due care to shareholders for the management of cybersecurity in line with the continually evolving threat posed by cyberattacks to the financial viability of the organisation. Cyber insurance remains a risk treatment but one that should support the remediation of cybersecurity incidents, if and when cybersecurity controls fail to mitigate the risk.

Cybersecurity regulation can have a positive impact on disrupting the cyber '*kill chain'*, potentially making it harder to take legal action against a board for failing to adequately apply cybersecurity. The implementation of cybersecurity regulation and associated risk management and controls makes it harder for cyber-attacks to succeed. The harder it is for cyber-attacks to succeed, the harder it is for hackers to profit from a successful attack and the more likely hackers will move on to target someone else, reducing the potential for boards to face lawsuits that otherwise could find that the boards have been negligent in their duties of protecting shareholder value.

References

1. *Left of Bang*, How the Marine Corps' Combat Hunter Program can save your life - Patrick Van Horne and Jason A. Riley (ISBN 978-1-936891-30-6).
2. Securities and Exchange Commission cybersecurity risk management, strategy, governance and incident response proposal - https://www.sec.gov/news/press-release/2022-39
3. The U.S DoD CMMC program - https://dodcio.defense.gov/CMMC/
4. DFARS 252.204-7012 - https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses#DFARS_252.204-7012
5. EU Network and Information Security Directive 2.0 - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN
6. EU Digital Operational Resilience Act (DORA) – https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554&from=EN
7. The White House proposed IoT cyber labelling - https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/11/fact-sheet-biden-harris-administration-delivers-on-strengthening-americas-cybersecurity/
8. EU Cyber Resilience Act (CRA) - https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act