U.S and EU cybersecurity regulation enforces 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 & Rachel Rose

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. 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. 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.

The need for cybersecurity compliance and cybersecurity risk management is not new, whether in the defense industry or for publicly traded companies. The Sarbanes Oxley Act of 2002[2] has long required cybersecurity compliance in relation to internal controls. And, in 2018, the U.S. Securities and Exchange Commission (SEC) published guidance which helped clarify two points:

1. "First, this release stresses the importance of maintaining comprehensive policies and procedures related to cybersecurity risks and incidents. Companies are required to establish and maintain appropriate and effective disclosure controls and procedures that enable them to make accurate and timely disclosures of material events, including those related to cybersecurity. Such robust disclosure controls and procedures assist companies in satisfying their disclosure obligations under the federal securities laws."
2. "Second, we also remind companies and their directors, officers, and other corporate insiders of the applicable insider trading prohibitions under the general antifraud provisions of the federal securities laws and also of their obligation to refrain from making selective disclosures of material non-public information about cybersecurity risk or incidents."[3]

On December 31, 2020, the DoD published *Instruction DoDI 5000.90 Cybersecurity for Acquisition Decision Authorities and Program Managers*. Policy, prescribing procedures, and management of cybersecurity risk by program Decision Authorities (DA) and Program Managers (PM) in the DoD acquisition process were established.[4] For DoD contractors, this is a material consideration.[5] It sets out the foundations for cybersecurity risk-based decision making within the Defense Acquisition System

[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] Sarbanes-Oxley Act of 2002, Pub. L. 107-204 (Jul 30, 2002).
[3] *See* SEC, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures* (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.
[4] *See* A. Watkin-Child, T. Dziekanowski, *DoDI 5000.90 – Its Impact on Supply Chain Risk Management (SCRM), Cybersecurity, and the Defense Industrial Base (DIB),* https://vimeo.com/554844535.
[5] *Id*.

(DAS), utilizing the RMF, which includes a Supply Chain Risk Management(SCRM) policy requirement for program managers.[6]

Traditionally organisations have been more reactive to the management of cybersecurity risk, adopting a stance of '*that won't happen to me*' ignoring the risk or relying on the purchase of cyber insurance to treat the risk, 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. Adopting a regulatory approach to cybersecurity, where the focus is heavily placed on the management of cyber risk. Regulation that includes the Securities and Exchange Commission's (SEC) cybersecurity risk management, strategy, governance, and incident reporting proposal[7]. The US Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC)[8] regime, focusing on the global Defense Industry Base (DIB), under Defense Federal Acquisition Regulatory Supplements (DFARS)[9]. The EU has released the Network and Infrastructure Security 2.0 (EU NIS 2.0)[10] Directive and the Digital Operational Resilience Act (DORA)[11], 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[12] or EU[13].

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 covered under the Securities and Exchange Act 1934. The DoD CMMC program roll-out timeline is unclear, but DFARS 252.204-7012 requirements for defence contractors to comply with NIST SP 800-171, are in place and enforceable. EU Member States have 21 months to convert EU NIS 2.0 and

[6] *Id*.
[7] Securities and Exchange Commission cybersecurity risk management, strategy, governance and incident response proposal - https://www.sec.gov/news/press-release/2022-39
[8] The U.S DoD CMMC program - https://dodcio.defense.gov/CMMC/
[9] DFARS 252.204-7012 - https://www.acquisition.gov/dfars/252.204-7012cdic-ir-safeguarding-overed-efense-nformation-and-yberncident-eporting.
[10] EU Network and Information Security Directive 2.0 - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&from=EN
[11] EU Digital Operational Resilience Act (DORA) – https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554&from=EN
[12] 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/
[13] EU Cyber Resilience Act (CRA) - https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

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

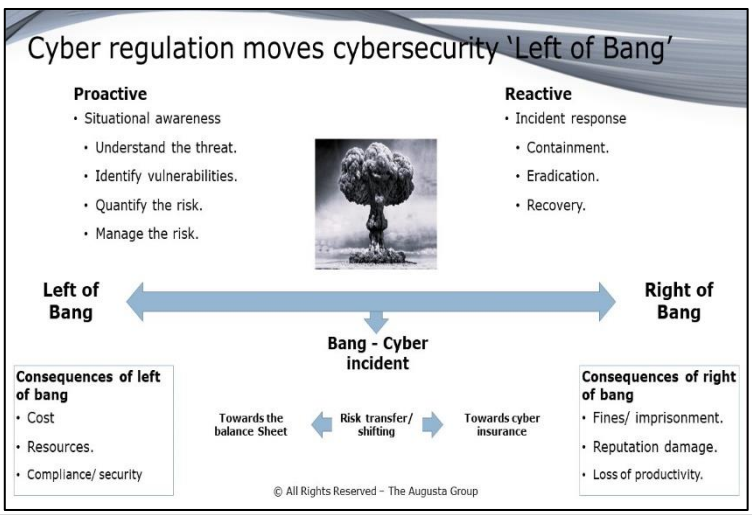
The results of current, pending and proposed cyber regulations will be to drive cybersecurity risk management compliance into the board rooms of covered entities. Boards should anticipate being required to implement a cybersecurity risk management strategy, governance, a cybersecurity risk management 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 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 the organisation's financial statements.

Cyber regulation will reduce 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 cyber insurance and the requirement to comply with cyber regulation, shifts the cost of managing cyber risk onto the financial statements 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 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, cyber risk management policies and procedures, cyber program, and updates to cybersecurity risk management if an organisations business strategy, financial outlook, or financial planning change. The 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. After the registrant determines that it has experienced a material cybersecurity incident. All of which requires an understanding of an organisations '*situational awareness'* as it relates to cybersecurity risk management.

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

Cyber regulation such as EU NIS 2, DORA and the SEC proposal requires boards to manage cyber risk. That raises the question '*can an organisation rely on cyber insurance as the sole risk treatment?*'. Given market conditions make cyber insurance expensive, with reduced coverage and exclusion clauses focused on nation state threat actors. The introduction of additional cyber regulations 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 risks, implementation of cybersecurity programs and cyber security governance, oversight, assurance, and attestation. In addition, regulators have been clear that boards must understand the impact of cybersecurity across their supply chains. Organisations should assure 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 the 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 oversight from risk, audit, cyber, legal and compliance committees. Necessitating the adoption of a three Line of Defence (3 LoD) model similar to that adopted by covered financial institutions, under the Basel accord. Cybersecurity risk

management compliance is a double-edged sword, failing to comply creates legal and compliance risk, while compliance necessitates situational awareness, 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 reporting. An approach that 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 that must be owned by a member of the board, who has the responsibility and accountability to oversight and assure risk. That could be the CEO, 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 cyber security program, they do not own enterprise-wide risk, and they are accountable and responsible for implementing the solutions to mitigate 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 that can take an objective view of risk management and compliance. Governed by the board and taking feeds from the various board reporting committees taking 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*' and a regulatory, compliance and legal risk that boards must face if they are a covered entity.
1b. Be clear over the obligations that cybersecurity risk management requires of boards to govern cybersecurity risks and oversight, assure and attest cybersecurity compliance.
1c. Be clear that cybersecurity is a strategic enterprise-wide business, not a technology risk. All functions and departments cross the organisation have a role to play in cybersecurity risk management.

1d. 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.

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

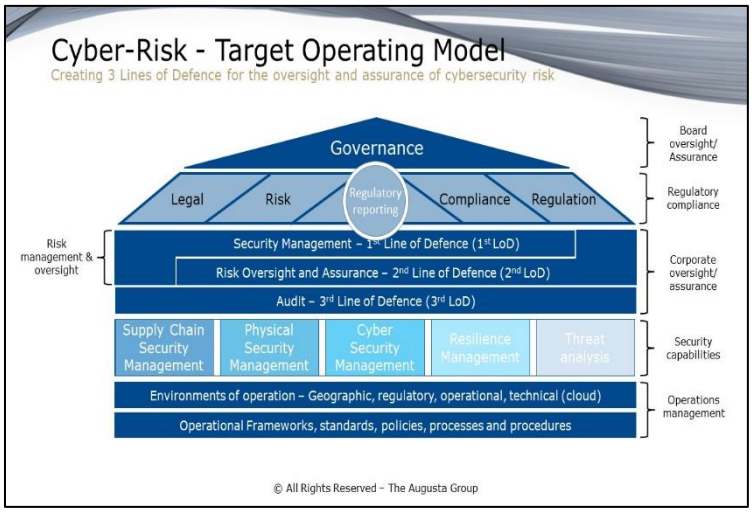
1f. Have a clear understanding of cyber regulatory and legal commitments across the jurisdictions their organisation operates.

Note: Boards should be clear about their legal commitments and put in place 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 compliance programs.

Step 2: Governance – Board oversight, assurance and attestation of cyber risk requires board governance.

Regulators expect boards to take an active role in the evaluation, oversight, assurance, and management of cybersecurity risks. That includes declaring the organisations cybersecurity governance, and the knowledge and experience the board of directors has in 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 board 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. So boards can provide a reasonable level of assurance that inherent risk, control effectiveness and residual risks are managed.

Step 3: Agree a 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 process and procedures and clarifies risk ownership, evaluation and mitigation and reporting.



An organisations internal and external stakeholders that include legal, compliance, regulatory, risk, audit, front, middle and back-office functions, and suppliers are accountable and responsible for the creation, management, oversight, assurance and

reporting of cybersecurity risks. Risks that the audit, risk, IT, Cyber, renumeration, strategy and operations committees coordinate, oversight, assure and report to the board executive committee.

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

Step 4: Compliance program. *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 controls (CIS). 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. That is required by cybersecurity risk management regulation.

Cybersecurity risk management compliance is structured by the TOM and delivered through a 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. 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.

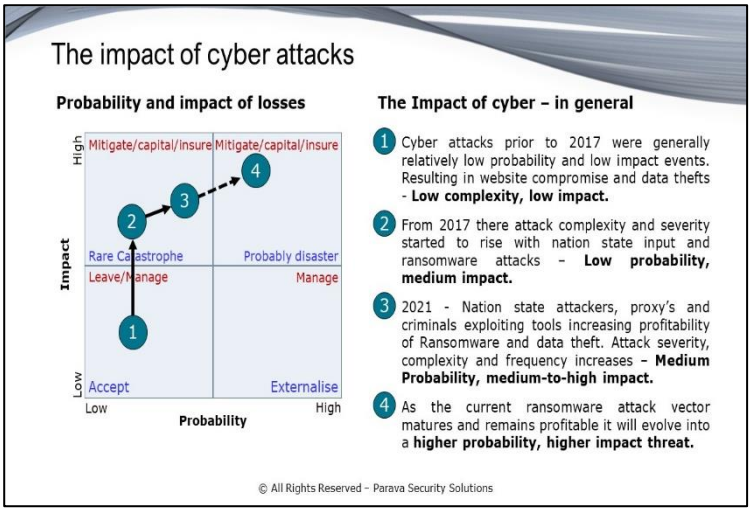
Step 5: Board oversight, assurance and reporting through Board committee structures – Board governance is a focus of U.S and EU Cybersecurity risk management regulation. Requiring board members to take an active role in the oversight and assurance of cybersecurity and risk management. Boards need to 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, HR and IT.

The TOM above sets out a 3 Line approach for cybersecurity that includes the identification, qualification, quantification, remediation and reporting of cyber risk. The potential penalties of failing to comply warrant an approach to oversight and assurance by board sub committees that could include the audit, risk, cybersecurity, IT, compliance, third party supplier and operations committees. Committees that feed oversight and assurance of cybersecurity risks to the board committee for final attestation, prior to submission of an agreed response to a regulator.

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 cyber security risk. The traditional approach for many to manage cybersecurity risks has been to rely on cyber insurance as the main form of risk transfer. For the 99% of organisations that are SMEs/ SMBs it is the only tool that organisations have to manage cyber risk. Cybersecurity is simply too expensive a risk to manage. The absence of cyber regulation has allowed boards to 'chose' to manage the risk; a choice that has been rightly based upon the economics of deploying cybersecurity and a perceived return. One influenced by the unlikely event of '*it happening to me'*.



This was based on cyber being a low probability low impact event. This is no longer the case, it is a risk that should be treated as a likely high impact event. It is a risk whose impact is considered by U.S Federal Government and the EU commission to be high enough, with such an impact, that they have seen fit to regulate cybersecurity risk management. In response to the concerns that cyber presents to the public and private sector, and the insurance industry has found difficult to manage. With ransomware being the predominant threat vector, cyber is a risk that will not be reducing until organisations take steps to manage the cyber risks. Steps that are now being enforced through regulation.

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 class action lawsuits. Costs that many organisations either self-funded or relied upon cyber insurance to cover. '*Left of bang*' costs are associated with implementing cybersecurity, governance, and the associated frameworks and practices for managing cybersecurity risk and controls. Traditionally organisations have found '*Left of bang*' costs too high, relied upon 'it won't happen to me', and cyber insurance to cover cyber incident costs rather than implement 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 skills 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 to the organisation's capital allocation. Cyber regulation requires boards to evaluate cyber risks below their historic levels of risk appetite ('it won't happen to me', use cyber insurance to treat the risk) and manage the 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. Managing 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 supports 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 cyber-attack, the more likely hackers will move on to target someone else. Reducing the potential for boards to face lawsuits that otherwise could find that they have neglected their duties of protecting shareholder value.