THE AUGUSTA GROUP

‘Left of bang’, the regulatory paradigm that drives cybersecurity risk management compliance ahead of cybersecurity and incident response.

Implications for boards and their security leaders

By: Andy Watkin-Child and Ted Dziekanowski

July 2022

Introduction - Left of Bang and Right of Bang.

The philosophy of the Augusta Group is to look outside of zones of comfort, knowledge, and experience to yield better solutions and results. In *'Left of Bang, How the Marine Corps' Combat Hunter Program can save your life[1]'* Patrick Van Horne and Jason A. Riley, describe the importance of situational awareness in combat. Risk management methodologies that are being proposed by regulators promote the concepts of situational awareness, as the means to managing cybersecurity risks.

Legislative and regulatory regimes proposed by U.S, EU and APAC regulators, are bringing the general concept of '*Left of Bang*' and '*situational awareness'* to corporate boards in the form of continuous monitoring and attestation of cybersecurity risk management. Regulators seek to address the gaps and failures of public and private sector cybersecurity and risk management compliance, as demonstrated by critical infrastructure cyber-attacks and ransomware. Boards will be held accountable for the oversight and assurance of their supply chain risks and their cybersecurity risk management strategy, governance, and incident disclosure, increasing their legal and compliance risks.

Regulators across the globe are setting baseline standards for cybersecurity risk management compliance, oversight, and assurance for boards of public registrants, Critical National Infrastructure (CNI) providers, Financial Institutions (FI) and their third-party suppliers. Organisations need to demonstrate appropriate management, oversight, assurance, mitigation, and reporting of cybersecurity risks equating to '*situational awareness*' of cybersecurity.

What is *Left of Bang*?

'Left of Bang – means before the bad stuff happens. That's where you want to be – alert, ready, prepared to respond to protect yourself and your loved ones.'

Historically cybersecurity management focused on incident management and reporting. The consequences being the misallocation of capital in pursuit of protection against cyber-attacks that have not had the desired effect on reducing their impact, as demonstrated by successful cyber-attacks that are increasing in complexity, frequency, and sophistication.

Developments in cybersecurity legislation, regulation, and enforcement, require adaptive risk management and organisations to demonstrate they are managing enterprise-wide cybersecurity risks, and those of their third-party suppliers. Achieved by identifying, assessing, treating, monitoring, and reporting cybersecurity risks with changes in business strategy, financial performance, and operations. Giving organisations the situational awareness (*left of bang*) that is required to demonstrate that they are managing their cybersecurity risks, before they materialise into '*bad stuff'*.

Bad stuff being the impact of a cyber incident on an organisation's stakeholders that includes customers, suppliers, investors, and staff. The impacts can range from a fall in share price, loss of investor confidence, incident remediation costs; legal, regulatory and supply chain risks; loss of contracts and jobs, to the loss of critical Intellectual property that impacts competitive advantage and national security (Controlled Unclassified Information).

What is Right of Bang?

'Right of bang – means after the bomb has gone off, after the shots have been fired, after the damage has been done.'

The predominant cybersecurity threat vector for many organisations is ransomware, which mostly occurs after data has been stolen. By the time a ransomware attack is found the damage has been done both to the organisation and its stakeholders. The impact of a ransomware attack includes reputational, legal, regulatory, financial and potentially supply chain risks rising exponentially. The transfer of these risks through cyber insurance is becoming much harder, with the rise in insurance premiums and the reduction coverage.

It is invariably more expensive to manage the consequences *Right of Bang,* than the costs associated with proactively addressing the causes of incidents *Left of Bang.* Managing cybersecurity risks before the *bang* is more economic and the consequences to national security easier to manage. Requirements that recent U.S, EU and APAC cybersecurity risk management legislation and regulatory enforcement regimes set out to enforce.

Driving towards '*Left of Bang*'

If you are working *Right of Bang*, you are waiting for the threat actor to strike first and you lose control of the situation. This creates a reactive state, that in the case of cybersecurity, the security professionals and board must be prepared and have the capability to deal with. Cyber-attacks are unpredictable and often chaotic unfolding potentially in directions they are invariably unprepared or experienced to manage.

'*Whoever strikes first possesses a powerful tactical advantage. When a person is right of bang, they are reacting to the action that took place……. Whenever a person is operating right of bang, it means that the enemy has the initiative and controls the situation. But operating left of bang requires intense concentration to identify the pre-event indicators and gain an advanced warning about the enemy's intentions. These indicators, however, are not always easy to discern. If the first time a Marine realizes a threat is present is when he sees an AK-47 assault rifle aimed in his direction, he has already lost the initiative and is now reacting to the enemy. Getting left of bang*

requires that he can make informed observations and build and enhance awareness of his surrounding'. – Patrick Van Horn and Jason A. Riley

Employing '*left of bang*' as a concept for cybersecurity risk management makes sense as it creates situational awareness throughout the risk management process. It can provide the board with appropriate information to make better more well-informed decisions as their organisational strategy, operations, financial performance, and regulatory requirements change. Situational awareness provides the capability to better prevent cyber incidents, and be prepared to react to attacks should they occur.

Focusing on regulatory compliance changes the economic paradigm for cybersecurity

In the case of kinetic conflict*, 'the larger we made vehicles, and the thicker we made armour, the larger and more deadly the insurgents made their IEDs……we were only treating symptoms, not the cause'*. A paradigm that was flipped on its head by the U.S Marines Combat Hunter Program and the concepts of '*Left of Bang'*. A program developed to focus on situational awareness and attack prevention rather than incident response after the '*bang*'.

No matter the threat, whether it is physical such as dealing with an IED or sniper attack, or a logical cyber-attack, proactive prevention is the most appropriate option. In both physical and logical attacks preventing an incident is more cost effective than dealing with the aftermath. However, prevention is complex, costly and situation dependent. Preventing the loss of life and damage associated with an IED attack, creates its own environment of operation and challenges for situational awareness. That are unique to every situation and can only be completely assessed at the time. But preparation '*left of bang*' provides a significantly greater chance of preventing the '*bang*', or better still managing the situation '*right of bang*'.

The costs of managing a cyber incident are well documented to be greater than the costs of managing cybersecurity. Cyber-attacks are unique to each organisation, where the costs of remediation include ransomware, legal, regulatory fines, lost revenue, lost sales, reduced profits and in some instances foreclosure. Recent cyber-attacks such as SolarWinds, Kaseya, Colonial Pipeline, JBS meat and Toyota demonstrated supply chain risks that increased the impact of silent cyber. Another example is the theft of DoD weapon system data and the poor standards of weapon system cybersecurity compliance, that were highlighted by the U.S Government Accountability Office (GAO) as far back as 2018[2,3]. Used, in part, to reinforce DoD DFARS[4] and CMMC regulations for the protection of weapon system Intellectual Property (IP), and in-part address the threat posed to U.S National Security.

The macro-economic impact of cyber-attacks on Critical National Infrastructure (CNI) and supply chains reaffirmed the reliance of the U.S. on corporate defensive cyber strategies, that are influenced by financial performance. Driving US presidential Executive Orders focusing on Supply Chain Security

(EO 14017[5]) and the Nations Cyber Security (EO 14028[6]) and U.S cybersecurity risk management regulation and enforcement regimes. Moving cybersecurity risk management '*Left of bang',* for prevention and situational awareness, based upon an understanding of enterprise-wide cyber risks rather than incident response. Regulations and regimes that other nation states are, or have, implemented.

Cybersecurity regulation is unintentionally driving a Left of Bang conversation

Cybersecurity risk management is a high priority for many regulators in 2022. The Securities and Exchange Commission (SEC) proposed amendments to its rules on 9th March 2022[7], recommending formalizing the disclosure of cybersecurity risk management, strategy, governance, and incident reporting by boards of U.S. public registrants; the Options Clearing Corporation (OCC) filed notice with immediate effect of proposed rule changes concerning the adoption of a cybersecurity attestation program in June 2022; U.S. Federal Government Agencies and their suppliers are required to comply with the Federal Information Security Modernization Act (FISMA[8] – 2002, 2014 & 2022) for supply chain risk management. The Department of Defence (DoD) requires Defence Industry Base (DIB) contractors and subcontractors globally to comply with DFARS 252.204-7012, 7019, 7020 and implement the NIST SP 800-171[9] cybersecurity standard. The EU reached provisional agreement on the text for Network Information Security 2.0 directive (May 2022[10]) detailing a suite of cybersecurity requirements that affect Critical National Infrastructure (CNI) providers. The EU Commission reached a provisional draft agreement on the Digital Operational Resilience Act in May 2022[11], requiring the governance, oversight, assurance, and incident reporting of ICT risk management by EU Financial Institutions (FI) and their ICT suppliers.

These regulatory regimes have similar requirements, and their impact extends beyond their national boundaries, impacting both national and international organisations. Driving cybersecurity *Left of Bang*, removing the impact of commercial market forces, and shaping compliance through regulation and enforcement regimes. These regulations require organisations to take appropriate steps to manage enterprise-wide cybersecurity risks, strategy, governance, and incident disclosure. Requirements that include, but are not limited to:

- Reporting cybersecurity policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity risks as part of its business strategy, financial planning, and capital allocation.
- Confirming Board governance roles for the oversight of cybersecurity risk. Detailing management's role in assessing and managing such risk, management's cybersecurity expertise, and management's role in implementing the registrant's cybersecurity policies, procedures, and strategies.
- Implementing a cybersecurity risk management framework and associated cybersecurity program.
- Reporting material cybersecurity incidents within four business days.

- Providing regulatory updates on cybersecurity risk management compliance and previously reported cybersecurity incidents.
- Undertaking independent testing of cybersecurity risk management compliance.
- Undertaking an independent cybersecurity assessment and certification before a DoD contract is awarded.

Regulatory enforcement

In October 2021 the U.S Department of Justice (DoJ) announced its Civil Cyber Fraud Initiative[12]. Making it clear that organisations that supply Federal Agencies could be fined under the False Claims Act (FCA,) if they fail to meet expected cybersecurity standards under contract. Recently tested in court with both the Comprehensive Health Services (CHS) and Aerojet Rocketdyne cases; Department of Treasury OFAC rules for ransomware payments[13]; Basel accords for regulatory capital for covered Financial Institutions; the Securities and Exchange Commission (SEC) and the EU Commission, are further examples of cybersecurity regulatory compliance regimes.

If the SEC cybersecurity risk management proposal moves ahead, corporate disclosures will generate noise in Capital markets that could result in investigations from the DoJ or the SEC. For example, Prime defence contractors that have reported their NIST compliance scores in SPRS as required under DFARS regulations, and completed a CMMC assessments will need to ensure comparative reporting to the SEC. Organizations that report their cybersecurity meets international standards, that subsequently undergoes a cyber-attack, may find they will have to not only report the incident in a timely manner but may undergoe closer examination of their cybersecurity risk management compliance. CyberSecurity risk management disclosures will also be useful for civil litigation, companies that are unfortunate enough to suffer a cybersecurity incident may find that their cybersecurity risk management, strategy, and governance disclosures are used to challenge their cybersecurity maturity reported to regulators.

Impact of cyber regulation on National and International organizations

Cybersecurity risk management has not been regulated with such breadth and depth by nation states prior to 2022. Cybersecurity risk management regulations will have a significant impact on National and International public and private sector organisations. Failure to comply to regulations such as the DoD DFARS and CMMC may result in fines or the loss of a DoD contract[14]. The SEC proposal has the potential to affect registrants on U.S capital markets, including foreign registrants. Affected boards will have to attest to cybersecurity risk management compliance and maybe used by market participants to make investment decisions and assess credit ratings. In the unfortunate event of a cyber incident regulatory submissions may not only be scrutinized by regulators but my impacted stakeholders as well. Likewise, DORA and the EU – NIS 2.0 directive stipulate similar requirements for cybersecurity risk management oversight, assurance, attestation, and reporting by EU Financial Services and Critical national Infrastructure organisations.

The regulators may set a high bar for cybersecurity risk management compliance, with standards likely to be higher than those that organisations may be required to comply with locally. For Example, DFARS 252.204-7012 requires DIB contractors to comply with 110 NIST SP 800-171 cybersecurity practices, compared to the UK cyber essential that requires 6.

The regulators require organisations to have a clear view of their enterprise architecture, which will include their cloud usage. Organisation will need to identify and assess threats and vulnerabilities, understanding the impact of cyber threats to their business model, build and manage a cybersecurity risk taxonomy to facilitate inherent risk assessment. Understand the most appropriate controls to reduce the risk (and impact), evaluate control effectiveness and evaluate cybersecurity residual risks. Put in place as much mitigation as the organisation can afford and think far enough ahead to understand the impact of cyber-attacks before they happen, so that boards are prepared to act. All of which, in our opinion builds the foundations to manage situational awareness, *left of bang*.

Life may get harder, before it gets better for security professionals

Unfortunately, for many organisations the historic lack of cybersecurity support and funding by the board room, has forced security professionals to prioritise cybersecurity solutions based on budget and not risk. That will change under cybersecurity risk management regulations, requiring boards and cybersecurity professionals to adopt risk management practices.

Cybersecurity risk management requires an understanding of the application of risk management frameworks, the application of cybersecurity standards, an understanding of business strategy, financial reporting, enterprise architecture, risk and control self-assessment (RCSA) to bring this disparate information together to evaluate cybersecurity risks. Boards need assurance that cybersecurity risks have been assessed, control effectiveness tested and there is a clear understanding of inherent and residual risk. Where there is residual risk the system security plan (SSP) will be updated and Plans of Actions and Milestones (POAM) documenting the process of risk mitigation. Ahead of internal and external audit evaluating cybersecurity risk management compliance, prior to board attestation. Boards who will be held accountable and responsible by regulators for managing cybersecurity. It is one thing to say that you are doing cybersecurity risk management, it is another to formally attest compliance and report your frameworks, standards, policies, procedures, risk assessment, POAMs and compliance to a regulator.

Cybersecurity risk management compliance, oversight, assurance, and board competency will be disclosed to investors and other market participants such as financial analysts, investment advisers and portfolio managers. Enabling them to assess the implications of cybersecurity maturity, risk management, board oversight and assurance, and the effects of material cybersecurity incidents on

short and long term financial and operational performance. That are likely to have a direct impact on investment decisions, credit ratings, cyber insurance premiums and share price.

Two notable compliance breaches in the U.S have highlighted the role of the C-Suite in decision making. The SEC recently bought charges against the Chief Compliance Officer (CCO)[15] of an organisation for his failings in managing regulatory compliance. The SEC recognized the importance of the role of the CCO in ensuring an organisation complies with Securities law and the need for a Chief Compliance Officer liability framework. The second follows the SolarWinds hack, the CISO has been highlighted by the court[16] as being the expert responsible to the board for managing cybersecurity. With a Civil lawsuit pending that aims to charge SolarWinds and its CISO for their failure in taking adequate actions to prevent the 2019 breach.

Conclusion

The regulatory approach to cybersecurity risk management compliance is in our view *left of bang*. It is being driven by regulators and enforcement programs, requiring organisations to implement cybersecurity risk management, and enabling situational awareness. Where once boards had an option to implement cybersecurity, they must now decide if they want to participate in a regulated market, they must implement cybersecurity risk management. Organisations that are not publicly traded should also be concerned, as they maybe suppliers of public firms that will be expected to understand and manage their cybersecurity supply chain risks.

The *Left of Bang* approach requires organisations to develop better situational awareness through an understanding of cyber risks along with a broader assessment of the enterprise-wide impact that cyber-attacks may have on organisations and its supply chains. Those cyber risks then being treated in a manner that could be considered adequate commensurate to the level of risk.

With regulation comes enforcement, eventually tested in court, which over time will set precedence and re-affirm compliance standards. Enforcement actions place corporate boards and security professionals on notice that their decisions could be assessed at a future date, in response to the decisions made in assessing cybersecurity risks, mitigating risks, and responding to cyber incidents.

Left of bang cyber regulation and enforcement may create challenges in the short term, but it may prove a positive opportunity moving forward, creating awareness of the challenges inherent in managing cybersecurity to the board room. Awareness of the challenges in establishing and funding the necessary governance to manage cyber risk may change the strategic planning for the management of cyber risk and information technology.

The change in the requirement for the management of cyber risk may lead to a migration to alternative solutions that provide risk awareness capabilities as a service and significant shift to

software development methodologies like DEVSECOPS which promote Kaizen like quality control and assurance prior to software being deployed. These solutions along with improvements in governance and better alignment of business objective to information technology can support the situational awareness that makes 'Left of Bang' a viable proposition.

References

1. *L*eft 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. Government Accountability office - Urgent Actions are needed cybersecurity challenges facing the nation
3. Government Accountability Office - Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities
4. DFARS 252.204-7012 - https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting
5. SCRM Executive Order - https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains
6. Cybersecurity Executive order - https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
7. Securities and Exchange Commission cybersecurity risk management, strategy, governance and incident response proposal - https://www.sec.gov/news/press-release/2022-39
8. Federal Information Security Modernisation Act (FISMA) - https://www.sec.gov/news/press-release/2022-39
9. NIST SP 800-171 - https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
10. EU Network and Information Security Directive 2.0 - https://www.europarl.europa.eu/thinktank/en/document/ EPRS_BRI(2021) 689333
11. EU Digital Operational Resilience Act(DORA) - https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/
12. Department of Justice (DoJ) Civil cyber fraud initiative - https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative
13. Department of Treasury Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments - https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf
14. DoD memo outlining penalties for failing to comply with DFARS cybersecurity requirement - https://governmentcontracts.foxrothschild.com/2022/06/articles/general-federal-government-contracts-news-updates/dod-memo-identifies-penalties-for-noncompliance-with-dfars-cyber-requirements/#more-1331
15. Settled administrative proceeding against Hamilton Investment Counsel LLC ("HIC") and Jeffrey Kirkpatrick - https://www.sec.gov/news/statement/peirce-statement-hamilton-investment-counsel-070122?utm_medium=email&utm_source=govdelivery
16. SolarWinds - https://law.justia.com/cases/federal/district-courts/texas/txwdce/1:2021cv00138/1122657/64/