Board and CEO Advisory

EVOLVING RISK IN THE EXISTENTIAL REALM

1 WHAT HAS CHANGED?

Over the past few years, strategic and significant risk for companies has evolved into an existential realm that must be identified early and managed effectively with new processes and tools for corporate survival. The aftershocks of the COVID-19 pandemic, economic instability, increased regulations, and other issues combined with technological change are leading to a seismic shift in the way many boards are approaching risk, strategy, values, and culture.

2 HOW IT MUST BE ADDRESSED?

In boardrooms today, directors must rely upon corporate counterintelligence and tailored business wargaming as a tool to gain advance warning of hidden risk (and new opportunities) for actionable resolution prior to crisis.

3 WHY THIS IS URGENT

Directors and CEO's are being held more accountable for strategic failures: this tool greatly reduces directors' increasing fiduciary exposure and increases their effectiveness in their role and career legacy.

CORPORATE COUNTERINTELLIGENCE

The Board's Role Has Shifted

Requiring Corporate Counterintelligence

Since 2014, board of directors have actively engaged in, and essentially own, the corporate strategy. Prior to that time, the board was in a far more passive role, and the need arose for a far more active involvement by the board. The behavior of boards was transformed. Now it is time for another shift in the way that corporate strategy looks at the evolving competitive landscape.

It has been long recognized that geo-economic factors have an enormous influence on how corporations will behave and survive in the future. However, today the activities of the various governmental and non-governmental “actors,” on the geo-economic stage, represent a huge part of the general risk profile of every business enterprise; and the private sector cannot rely on government to manage or even identify those risks. In fact, even simply identifying all the relevant visible and hidden risks, that can have a significant impact is very challenging and requires focused effort and specialized expertise.

Today, all risk, including strategic risk, operates in an environment of permanent geo-economic chaos. Businesses are locked into antiquated risk processes and assumptions that are obsolete in providing an effective baseline for current and future decision-making. The hyper advancement of geo-economic risk for companies requires new methods for managing all risk, including elevating Cyber as a strategic risk.

A disturbing trend has developed in which foreign intelligence services, nation-state actors, and criminals are using intelligence collection techniques against American companies to steal valuable trade secrets and assets. This activity can bankrupt a company by compromising years of costly research and development, weakening the U.S. economy, and threatening national security.

Corporate boards and executive officers must understand and manage the true increased threat their companies face. Many are currently engaging this fact. It is one that has evolved beyond the stage where information security, and Cyber as one example, can simply be delegated to the CSO or CISO - it requires full executive engagement focus. With the tools now available to adversaries, the American private sector is more vulnerable than ever.

Proper response requires a top-down culture shift in the enterprise and the supply chain that align risk, strategy, IP, technology, Cyber, and security, with your most important asset - the human factor. A culture shift begins with corporate counterintelligence (CCI). Corporate counterintelligence refers to leveraging intelligence from adversaries to protect your company’s intellectual property and sensitive data from unauthorized access, infiltration, sabotage or theft across the enterprise and the supply chain.

An effective CCI program ensures your company has an unbiased process to identify its most vulnerable assets, scans and understands the threats to those assets, has discovered the hidden vulnerabilities that make your company susceptible to exploitation, and has taken the appropriate execution to mitigate risks.

TAILORED BUSINESS WARGAMING

Corporate Counterintelligence, while essential, must be coupled with a dynamic tool to apply it to the enterprise and supply chain for execution and adoption. It provides the ability to reveal hidden risk in advance and the ability to quickly pivot out of risk and into new opportunities.

Since the 1800's, wargaming proved indispensable to our military. Today, wargaming adapted to business is a necessity for corporate survival in the evolving geo-economic environment of chaos. Tailored Business Wargaming (TBW) is dynamic by design and tailored to each company, executives, products, strategy, markets, competitors, suppliers, and adversaries through an intensive four week 'deep dive' into the company and its environment.

TBW encompasses all risk including financial, reputational, Cyber, operational, compliance, legal, geo-economic, mergers and acquisitions, supply chain, decoupling, health crises, location hazards, and others. It solves the problem: "I don't know what I don't know" and to "see around corners" with advance warning to aid successful execution and risk mitigation throughout the enterprise and supply chain.

When fused with Corporate Counterintelligence, TBW is a powerful executive leadership tool with the ability to discover hidden risk and new opportunity, in advance, while providing an action plan for ownership and execution. The process aligns executive leadership and the human element with forward-looking strategic risk and strategy.

Other wargaming methods for business remain outdated and significantly inferior. "Off the shelf" static wargames fail to be truly tailored or dynamic in embracing the company in this rapidly changing environment or have the depth required for discovery and positive change. Their design is closed in search capability which limits scope, actionable results, and the ability to reveal hidden risk.

Note: Tailored Business Wargaming operates at the strategic layer with an 'open search' capability and must not be confused with Cyber red teams or limited tabletop exercises.

Most companies use TBW across the top levels of leadership and management including the supply chain, then rollout a half-day summary to the enterprise for the ability to pivot through a common communication platform.

FBI AND MI5 DIRECTOR'S REMARKS TO GLOBAL BUSINESS LEADERS IN LONDON (07.06.2022)

Key Points: "The Chinese government poses an even more serious threat to Western businesses than even many sophisticated businesspeople realize. So, I want to encourage you to take the long view as you gauge that threat and as you plan to meet it.

The Chinese government is set on stealing your technology - whatever it is that makes your industry tick - and using it to undercut your business and dominate your market. And they're set on using every tool at their disposal to do it.

Consider that it may be a lot cheaper to preserve your intellectual property now than to lose your competitive advantage and have to build a new one down the road.

Where we see some companies, stumble is in thinking that by attending to one, or a couple, of these dangers, they've got the whole Chinese government danger covered—when really, China just pivots to the remaining door left unattended.

The Chinese Government sees Cyber as the pathway to cheat and steal on a massive scale.

But in addition to traditional and Cyber-enabled thievery, there are even more insidious tactics they'll use to essentially walk through your front door - and then rob you. The Chinese government likes to do this by making investments and creating partnerships that position their proxies to steal valuable technology.

Chinese companies are owned by the Chinese government - effectively the Chinese Communist Party. But the problem is bigger than that China often disguises its hand in order to obtain influence and access where companies don't suspect it.

Just as in Russia, Western investments built over years could become hostages, capital stranded, supply chains and relationships disrupted. Companies are caught between sanctions and Chinese law forbidding compliance with them.

And if China does invade Taiwan, we could see the same thing again, at a much larger scale.

That's not just geopolitics. It's business forecasting.

As I've heard one business leader put it recently, companies need to be wrestling with the strategic risks China poses to their growth in the long-term - and thinking about what actions they can and should be taking now, to prevent catastrophe later. I know this all sounds alarming. But while the threat is immense, that doesn't mean harm is inevitable.

"Full Press Release: https://www.fbi.gov/news/speeches/directors-remarks-to-business-leaders-in-london-070622?utm_campaign=email-Daily&utm_medium=email&utm_source=executive-speeches&utm_content=%5B1441346%5D-%2Fnews%2Fspeeches%2Fdirectors-remarks-to-business-leaders-in-london-070622

BLACKOPS PARTNERS

T. CASEY FLEMING

Chairman and CEO, BlackOps Partners Corporation
www.blackopspartners.com
contact@blackopspartners.com