ARTICLE

CYBER-SECURITY AND AI CHALLENGES FOR CORPORATE BOARDS

Enablers of transformation and competitiveness can also become existential threats

Prof. Colin Coulson-Thomas
President, IMS and Director-General, UK & Europe
Institute of Directors (IOD), India

Contemporary boards are confronted with multiple and inter-related risks. For the fifth year in a row, cyber incidents were regarded as the top business risk by respondents to Allianz's 2026 Risk Barometer survey. AI is the biggest riser in this year's annual survey. It jumps from tenth to second place after cyber issues, highlighting the emerging risks for companies in almost all industry sectors. Confronting cyber and AI risks and threats is a strategic issue for corporate boards and an operational concern for business executives.

Cyber capabilities and AI are used individually or together for both attack and defence. They can be used to disrupt, discredit, impersonate, infiltrate, subvert, extract a ransom, prevent continuing operation, weaken or destroy.

Companies and countries are at risk, along with the infrastructures and services upon which they depend. AI, initially promoted as an enabler of competitiveness and transformation, has emerged as an existential threat, including to human primacy as it develops, escapes human control and boosts the growth of other serious threats.

Cyber and AI risks and threats are not hypothetical. For many people and organisations, they are a daily reality, active and rapidly evolving. Bad actors, whether criminal for financial gain, state supported for grey zone purposes, terrorist to further a cause, or a combination of them have moved on. As barriers to entry fall, the cost of mounting AI enabled attacks can be more affordable. Legislation and regulations fall further behind. Delays in securing agreement and funding for responses persist. Cyber security is now often relative and elusive.

Cyber Vulnerabilities and Precautions

Businesses experiencing sustained attacks and likely targets should identify what is critical for achieving their mission or purpose and ensure backup and recovery arrangements are in place. Prudent players assume critical systems will be penetrated. They are ready to provide alternatives that can be quickly activated and scaled up. An analogue back up for the delivery of an essential service is advisable. If well-equipped and prepared assailants achieve their objectives, a worst-case scenario could be a likely rather than a possible outcome.

Safety and security vulnerabilities remain in evolving AI capabilities. The ability of AI models to escape human control is accelerating. They have been found to cheat and escape the constraints of an intended secure environment to search, hack, find and write or execute code externally. They mirror people who use questionable means to achieve their aims. Deepfakes can be used to imitate a trusted person. Prioritising growth over security increases vulnerabilities. Not wanting to be left behind can fuel AI adoption before their consideration.

Changes to governance arrangements, systems, processes and business models, transition and transformation journeys, reshaping markets and new models of operation and related innovations may create more points of vulnerability and additional access routes. Criminal and malevolent actors can use AI and other applications of technology to penetrate and exploit them while boards discuss cyber strategy and policies prior to their adoption at future meetings and requests for funding. Risk assessments should include cyber and AI risks.

Responding to Cyber Attacks

Basics such as avoiding unnecessary internet exposure and the use of multifactor authentication are sometimes overlooked. Could systems be run without being connected? Keys to survival are early detection, duplication and back up arrangements, stand-alone critical systems, quick recovery processes and alternative models of operation to maintain core services. Trusted and competent collaborators are scarce. Collaboration with trusted law enforcement agencies and the prospect of a response may deter attacks on some entities.

> Directors walk on eggshells. Dilemmas are linked like never before. Opportunities come with risks and can be accompanied by existential threats, for which people, organisations and societies are ill-prepared.

Defensive measures should be risk-based, proportionate and justifiable. Human oversight of autonomous AI agents and employing them for less important tasks is advised, lest they stray beyond foreseen limits. By the time a cyber-attack is verified it might be too late to avoid harm. The focus may have to be prevention of further spread, recovery, learning from events and the experience of others, and collaboration to be better prepared in future. Previous expectations about the integrity and objectivity of critical software may not apply to AI.

Technology companies are powerful vested interests. They could do much to increase cyber security, but lobby governments and put the case for removing regulatory barriers and allowing them maximum freedom to operate, innovate and be competitive. Companies operating internationally encounter different country approaches, ranging from those that are market led to the relatively tight regulatory framework of the EU. Data protection and its authentication, doctoring and misuse are becoming critical issues for many companies.

Redefining Infrastructures

Many boards should think differently about infrastructures which may need to be reshaped or reinvented to be more resilient to assault and better suited to future requirements. At a national level, critical infrastructure can face repeated cyber-attacks and sleeping malware may already be in place. The high vulnerability of electricity grids and other infrastructure, including payment systems, suggest they should feature in national security strategies. Those responsible for cyber safety and security at country level face multiple claims on their time.

Cloud platforms and sectors such as defence, energy, space, telecommunications and infrastructure, advanced engineering and technology, and related entities may be attacked by state-actors looking for opportunities to disrupt, erode confidence, infiltrate to create future denial of service opportunities, and/or steal intellectual property which might be accessed via an academic collaboration. Energy networks could already be under stress due to accelerating demand from mega data centres required to support rapidly spreading AI use.

Public bodies and utilities can be at risk of attack from criminal and state actors because of their reach, the data they hold, the damage disruption might cause and/or the

> Critical infrastructure can face repeated cyber-attacks and sleeping malware may already be in place.

possible scale of ransom demands. Legacy systems and codes are especially at risk. Red teams could be asked to identify those which are most vulnerable. Liberal democracies are especially susceptible to misinformation and disinformation, and the full spectrum of hybrid warfare attacks. Their autocratic adversaries aim to sow division, undermine trust and discredit public authorities.

AI at an Inflection Point

Siren voices champion AI. Its use seems addictive. Its adoption and spread have been rapid. Countries strive for AI leadership. Some dream of world domination through AI. Initially hyped by developers, vendors and consultants sensing opportunity, AI now divides opinions among its creators, public and regulators. Benefits come with risks. Investment in AI and the mega data centres which enable it crowds out that in technologies that are or may be critical for national security, sustainable growth, or addressing existential threats like climate change.

AI advances so rapidly that loss of human control seems likely. Attempts at regulation in a divided world seem destined to forever lag and be easy for it to avoid or evade. AI use may discriminate, lead to disastrous outcomes, or deliver erroneous and misleading advice. It can enable autonomous devices to seek out and eliminate human life. It could supercharge the development of biological and chemical weapons and is used across all armed services to speed detection and increase kill rates. Autocrats use it to identify and eliminate opponents.

We may be at an inflection point. AI Impact Summits have been concerned with responsible collaboration and adoption of enabling technologies for inclusive, socially beneficial and sustainable outcomes. Mega data centre demand for energy and water can increase prices and render some areas uncompetitive. Opposition to data centres is growing on health, economic, environmental and social grounds. Ensuring human oversight and control is becoming more challenging and a diminishing prospect. Divisions make whole of society responses unlikely.

Recalibrating Corporate Boards

A board should review a company's cyber risk profile, resilience and vulnerabilities, and ensure its people understand the importance of anticipation, awareness, preparation and vigilance. Precautions should also embrace contractors, customers, suppliers and supply chains and damage limitation measures. Open-source software can house malicious code, which may also exist undetected in critical safety, security and service applications. Tools can contain sleeping features. Response times and collaboration may need to be stepped up.

For many boards, the emphasis is shifting from protection of physical and intellectual assets to ensuring the continuity of services. Cloud data and the internet could be unavailable after a combination of cable cutting and cyber-attack. Directors should ensure a board's focus, oversight, understanding and vigilance are appropriate for the sector or sectors, contexts and locations in which a company operates. AI use should be ethical, considered and justifiable. A board's awareness, skillset and modus operandi must be appropriate for changing realities.

Directors walk on eggshells. Dilemmas are linked like never before. Opportunities come with risks and can be accompanied by existential threats, for which people, organisations and societies are ill-prepared. Few if any would know how to cope if a combination of them occurred simultaneously. Responsible leaders should act to ensure any possible short-term gains from how AI is used, by whom and for what purposes, are reconciled with longer-term sustainability and our collective and planetary resilience, safety, security and survival. ■

Prof. Colin Coulson-Thomas holds a portfolio of leadership roles and is IOD India's Director-General, UK and Europe. He has advised directors and boards in over 40 countries.