



# Directors, Boards and Cyber Security

## Understanding and Preparing for Evolving Threats

Companies face a widening range of cyber threats from a variety of criminal, state and non-state actors. Combinations of them may work together. Greater connectivity and the delivery of services electronically increase exposure to cyber-attack. Malicious activities may also be undertaken by autonomous actors and systems and supercharged by quantum technologies. Step changes in preparedness, resilience, response times and collaboration are needed.

Changes to governance arrangements, systems, processes and business models, transition and transformation journeys, and related innovations create additional access routes and more points of vulnerability. Criminal and malevolent actors can use AI and other applications of technology to penetrate and exploit them while boards are still discussing cyber strategy and policies prior to their adoption at future meetings.



**Prof. Colin Coulson-Thomas**

President, Institute of Management Services  
and Director-General, UK & Europe  
Institute of Directors, India

“

Resilience and preparation for cyber risks and threats should embrace organisations and their people, along with contractors, customers, suppliers and supply chains.

A corporate and/or country focus on growth and/or competitiveness may lead to pressure to acquire and use applications for their hoped-for contributions, without the delays that more meticulous evaluation might require. This can expose organisations to cyber and other risks. Many companies do

not have the scale, means or know-how to impose sufficient costs and risks upon attackers to deter their attempts to infiltrate and cause harm.

### Cyber-crime and Threats

Cyber-crime can be financially rewarding for those whose technical prowess exceeds that of their victims. Scammers and ransomware attackers only need a small proportion of assaults to succeed to extract large sums of money from big enterprise prey. Scams include the use of impersonation to lure people onto WhatsApp or social media groups for investors where they can be taken advantage of. Those who suffer loss can be at risk of being defrauded again.

The threat landscape is continually evolving. Increasingly there are also extremist and ideologically motivated individuals to contend with. Dangers may be posed by unknown radicalised actors with axes to grind, or terrorists burning with a cause who are not on the radar of law enforcement agencies. Barriers to entry for potential assailants are falling, and the cost of mounting attacks that may be AI enabled is becoming more affordable.

Scammers are getting more sophisticated and convincing as they learn more about what works best and vulnerabilities. The use of AI and other tools can speed up this process, create fake images and videos, and spread misinformation and disinformation. There are often too many potential threats for national authorities to effectively monitor. They must be selective.

### Assessing Vulnerability

Certain companies invite attention and can attract different attackers. Criminals may target financial services, but they along with utilities, cloud platforms and sectors such as defence, energy, space, telecommunications and infrastructure, advanced engineering and technology related entities may also be attacked by state-actors looking for opportunities to disrupt, infiltrate to create future denial of service opportunities, and/or steal intellectual property.

Prioritising growth over security can increase vulnerability. Technology companies that could do more to increase cyber security as a public good lobby governments and put the case for removing regulatory barriers and allowing them the maximum freedom to operate, innovate and be competitive. Companies operating internationally encounter different country approaches, ranging from those that are market led to the regulatory framework of the EU.



Prioritising growth over security can increase vulnerability.

Data protection and its authentication, doctoring and misuse are becoming critical issues for many companies, along with the integrity and objectivity of software upon which they depend. Open-source software may be more vulnerable to the implantation of code designed to serve the interests of hostile third parties when required. Such code may exist in critical safety, security and service applications, without companies and their boards being aware of the risks. Tools may be bought and used by people who are oblivious of their source.

### State-sponsored Attacks

Authoritarian states are increasing their use of cyber and other onslaughts to undermine democracy and democratic countries. They are becoming bolder and more ambitious in their attempts to disrupt, discredit, sow division and undermine. More opportunistic attacks may be state funded and undertaken by agencies of the state in collaboration with criminal groups. Quick reactions and counters to the aspirations of certain state actors may be required.

As geopolitical disputes unfold, state sponsored attack priorities can switch from longer-term attempts to subvert to more overt but deniable efforts to disrupt by grey-zone or hybrid-warfare activities such as cutting cables by dragging anchors. Globally operating companies should monitor evolving events and ramp up their contingency and recovery arrangements.

It may benefit those seeking to erode confidence and trust and disrupt relationships and supply chains, to increase insecurity and uncertainty and trigger costly reactions and responses. Malevolent actors in one category may pretend to be in another, where and when they judge this might be beneficial. Monitors and defences are not always sure of who they are dealing with. Intentions may be different from articulated aims.

### Responding to Attacks

Defensive measures should be risk-based, proportionate and justifiable. By the time successful cyber-attack costs are verified and known it may be too late to prevent the harm caused. The focus may need to be prevention of spread, recovery, learning from events and the experience of others, and collaboration to be better prepared in future.

General advice can be provided, such as not giving personal, financial, corporate or other information to unsolicited approaches from those offering to help or protect, blocking their initiators from further contacts, and only scanning QR codes from trusted sources. People should be wary of approaches via social media, situations where they feel under pressure to act, and offers of help in recovering a loss or dealing with unauthorised access.

Keys to survival are early detection, multiple duplication and back up arrangements, stand-alone critical systems, and/or alternative models of operation to enable greater resilience and maintain core services, and quick recovery processes. Collaboration with trusted law enforcement agencies and the prospect of a response, may deter an attack on some entities.

### Involvement of Directors and Boards

Boards should provide strategic direction. They should assess whether a CEO and key players are alert, anticipating, preparing, vigilant and addressing realities, or preoccupied, ignoring possible scenarios and largely reactive. A key question is whether they have the bandwidth to anticipate dangers such as hidden prompts within an email causing an AI agent to delete data, make fraudulent or embarrassing transactions, or initiate links to other targets.

Key executives may lack the imagination to foresee what could happen, including to services, infrastructure and data centres on which operations depend, or what other entities a company might provide access to if penetrated. Directors should ask 'what if' questions to assess awareness and understanding of possible assailants, sleeping malware, new arenas of exposure and sources of

risk, and capability to effectively respond, operate and recover.

Some directors and boards might be in denial of cyber risks and threats. They may consider them technical matters rather than strategic issues that require their attention. In house cyber security teams sometimes struggle to gain access to them. As a chain is only as strong as its weakest link, the corporate equivalent of a whole of society approach is increasingly needed.

### Inhibitors of Effective Preparation and Response

Directors and boards sometimes walk on tight ropes when stakeholders and wider publics are unaware of how they might be affected by cyber and other dangers, risks and threats. In terms of resilience, many boards seem oblivious to grey zone and hybrid warfare threats to systems and infrastructures at times of heightened tensions. Major companies may lack the means of continuing operations in an analogue world when digital services are blocked or unavailable.

Concerns about collusion may discourage, inhibit or prevent collaboration with other entities to strengthen collective cyber defences, if sharing certain information might be viewed as anti-competitive. Reactions to heightened risks and warnings can sometimes be delayed because of concerns about alarming customers or unsettling stakeholders. They might be viewed as disruptive of relationships and seen as inconvenient by those unaware of the risks.

### Anticipation and Forethought

Within large and internationally operating companies, cyber defence responsibilities can be widely dispersed and available resources thinly spread. Few arrangements may exist for active responses, or the equivalent of 'fighting back'. In contrast, attackers can concentrate their efforts at weak points and quickly exploit where and when access is secured. Entering the mindsets of potential or likely assailants may enable points of attack to be anticipated.

One could also anticipate where some categories of assailant might wish to go once inside a corporate network. Preparedness could involve damage limitation by erecting barriers, creating distractions and closing off entry to various subsystems. Reducing connectivity with separate entry requirements to self-contained subsystems might increase security, but inhibit collaboration across business unit, discipline, functional, work group and entity boundaries.



Boards must be realistic in their understanding of the extent of disunity, division, polarisation and opposition that exists in societies and countries in which they operate, the capabilities of local, regional and national law enforcement agencies, who can be trusted, and the cooperation and responses required to deter attacks.

Resilience and preparation for cyber risks and threats should embrace organisations and their people, along with contractors, customers, suppliers and supply chains. Some participants in corporate networks of relationships may be more vulnerable than others, and/or more likely to be attacked. They should be identified. Technical solutions alone are unlikely to be sufficient as various human and governance factors can increase exposure and vulnerability.

#### Encouraging Wider Engagement

Concerned boards can put the case at local and national level for devoting more resources to the protection of infrastructures and vital services, and efforts to limit radicalisation and combat extremism. Comparing assessments may identify the same and/or similar likely suspects and help to align preparation, defences and counter measures. All employees, contractors, and citizens should be encouraged to be vigilant 24/7, including when off-duty and relaxing, and especially overnight, at weekends and on bank holidays.

Where there are ways of reporting frauds and malicious attacks, many people and organisations are reluctant to do so. Much of the harm they cause is hidden. More effort may need to be devoted to cyber-related communications and enabling learning from others who are willing to share their experiences, especially those more likely to have experience of types of attack which are likely to increase, such as to utilities in 'front line' states.

Engagement with local networks may help to increase vigilance within communities from which employees are drawn. At a national level, a board may have a view on regulation of the use of AI and technologies which can be weaponised, limiting misinformation and disinformation that undermine trust, preventing alienation, crime and the growth of disgruntled groups, and increasing national and international collaboration. Certain companies might have a role to play in national resilience and security.

#### Addressing Realities

Security, secrecy and control are increasingly transient, at risk or an illusion. Companies remain vulnerable to access via alienated and disgruntled insiders, the private devices, tools and homes of employees and contractors, and the greater vulnerability of legacy systems and many small business suppliers.

Hostile state actors may already have prepositioned or reconnoitred access to utilities and other critical systems so that they could be 'turned off' in crisis situations. They may also be able to listen to conversations that are not encrypted to the advantage of their own national competitors of targeted companies.

#### Identifying Potential Collaborators

Boards must be realistic in their understanding of the extent of disunity, division, polarisation and opposition that exists in societies and countries in which they operate, the capabilities of local, regional and national law enforcement agencies, who can be trusted, and the cooperation and responses required to deter attacks. Continuing corporate resilience can depend upon access to the technologies and expertise needed to remain current. This may require greater collaboration between industry, academia and government.

Addressing the full range of risks and threats can require timely, serious and productive collaboration. Across jurisdictions, some law enforcement agencies are more integrated than others, and Governments vary in the extent to which they are proactive or reactive and engaged in the cyber equivalent of an arms race. For the more aware and better prepared cyber defence could become a shared purpose. Boards should prioritise 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.**