ARTICLE

CONFRONTING CYBER RISK REALITIES

An Overview of Contemporary Threats and Governance Requirements

*Prof. Colin Coulson-Thomas
President, IMS and
Director-General, UK & Europe, IOD India

Addressing cyber challenges, risks, and threats requires awareness, preparation, and individual, corporate, and collective action to protect identity, prevent fraud, and enhance security. The number, range, and sophistication of attacks are such that while only a small proportion of them may succeed, this might be enough to fund the continuation of malevolent activities according to the business models of attackers, some of whom may also be partly or even wholly motivated by non-financial goals. Future trajectories and defences are uncertain.

Directors and boards should understand the various dangers and threats that people and organisations face, who they are up against in terms of their possible perpetrators and assailants, the methods they use, and how these might be countered. They need to be aware of who and/or what confronts them today, their possible motivations, and who and/or what they may have to contend with in the future. There are issues that boards should address and options to consider. Both tactical and strategic responses are required.

Understanding the range of cyber threats

Cyberattacks can be undertaken for various reasons, and they may have multiple objectives. Some attacks may be made by criminal gangs primarily for financial gain or by other bad actors to fund cyber activities in furtherance of higher-priority objectives. Financial gains can be made by theft following impersonation, the implantation of ransomware, or some other deceit. Understanding sponsors and perpetrators and their motives can yield clues as to purpose, future intentions, and whether a victim is an intermediary or the final target.

Denial-of-service attacks could be undertaken for financial gain or by a state actor or proxy to undermine and/or damage another state. These ends could also be achieved by a disc-erasing wiper malware attack. The intended target could be one or more suppliers of services, those who rely upon them, or those to whom they might complain or feel accountable. The motive could be to unsettle, disadvantage, distract, weaken, inhibit, deter, prevent, probe, damage or destroy, erode confidence and trust, or favour an alternative or competitor.

An early attack could be exploratory, a form of reconnaissance undertaken to assess how alert a target is, the nature of reactions, and the time taken to respond, which may suggest windows of opportunity. Some attacks might go undetected, creating options for the perpetrator to consider how best to take advantage of this situation. Risks and threats are continually evolving, as with almost every change or development, there are likely

> Improving protection and decreasing the impact of breaches may require doing things differently. Serious thought may need to be given to reducing connectivity and separating and duplicating systems, especially critical ones.

to be malevolent units looking for possible vulnerabilities and considering how to take advantage of them.

Realising the enormity of the challenge

The strategies of different categories of attackers vary according to their motives, capabilities, and business models, who and what targets they are up against, the precautions and defences they encounter, and their growing experience of what works. They might have an opportunity to learn from a much greater number and variety of cases than those who are just focused on defending a particular system or entity during their working hours. Attackers may better share what they have learned and be less constrained by rules, policies, and norms.

Cyberwarfare can be asymmetric and/or unequal. While attackers may be unknown and difficult to identify, they might find it relatively easy to learn a great deal about their targets, either individually if they are high value or as a category if they are playing a numbers game. The habits and routines of people and the processes and practices of organisations that their staff, customers, suppliers, and partners are expected to observe make them vulnerable and slow to adapt and change. Predictability, uniformity, and conformity can all increase risk.

The cyber strengths and weaknesses of different sectors and businesses within them vary. Some of them can be especially vulnerable. Financial services providers, their clients, and their interrelationships can be priority targets of bad actors seeking financial gain. Intellectual property, other forms of know-how, business intelligence, and trade secrets could be the subject of commissioned thefts. When related to armaments, national security, and defence, an assault might be state-sponsored and/or undertaken by a non-state actor or proxy.

Recognising the unequal positions of assailants and guardians

Democracies and democratic institutions, positions, and players can find themselves under continuous attack from authoritarian regimes, whether to discredit, undermine, or sow division. Active attempts might also be made to degrade critical infrastructure. Increasingly, misinformation, disinformation, and fake news are used to encourage dissent, support hostility toward democratic principles, and favour authoritarian values or perpetrator policies. Undermining trust in the media and compromising communications can sometimes cause great harm.

While businesses at risk and the victims of malevolent cyber activity are likely to focus on and prioritise their individual corporate situations, the police and criminal justice system may take a wider and more systemic view. Given resource constraints, they may have to prioritise which cases to investigate and whom to protect and/or prosecute. They may also have a limited remit in relation to the geographical area in which they can operate. Available resources can rarely be easily deployed against overseas and state-sponsored perpetrators of cybercrime.

Criminal gangs and state and non-state proxy actors are less limited and may face a few restrictions. Operating digitally, they can target likely victims wherever they may be, and as one telephone line, email address, or website becomes compromised, they can quickly switch to another. Their existence may be evident, and their 'signature' apparent in their modus operandi. However, their flexibility and speed of adaptation make them difficult to trace and often almost impossible to bring to justice when they have foreign state support.

Identifying areas of vulnerability

Many of those who engage in malevolent activities benefit from the help of one or more insiders within their victims. Corruption is widespread. It can be found almost

wherever there are people, and it is endemic in many developing countries and in certain parts of the world. Motivations to harm an employing and/or accessible organisation, can range from personal and financial issues to a desire for redress or revenge. Resulting actions may include cybercrimes undertaken for financial gain, to cause harm or support a cause, or for other reasons.

Directors should face the reality that within their companies, there may be people who, for various reasons, are disgruntled or in need of money and who will take advantage and obtain a benefit by doing something they know to be wrong and detrimental to some if they feel they could get away with it. For a proportion of people, the issue may be one of price in relation to risk rather than a matter of ethics, principles, and values. They may be helped by colleagues who leave devices running when away and fail to observe security protocols.

Staff should be alert to possible warning signs, such as people working late, not taking holidays, or changes in circumstances, habits, or access to different systems. Many traditional and paper-based systems and processes are both insecure and inefficient compared with digital alternatives. However, the latter and the technologies and infrastructure upon which they depend are themselves vulnerable to interruption, attack, and denial. The internet could be taken down by natural events and certain actions by malevolent actors.

Protecting identity and reducing fraud

Impersonation can be a doorway to cybercrime and fraud. A priority for many people and organisations is to protect their digital identities. The quality and security of digital identity infrastructure, how it keeps pace with digital developments, and data protection, regulatory, and compensatory arrangements can vary by country. A company that operates internationally should take cybersecurity considerations into account when deciding where to locate data centres and certain activities. Various scenarios and contingencies should be tested.

Fraud protection practice and arrangements for supporting the victims of fraud also vary by jurisdiction. On occasion, certain directors, companies, corporate officers, executives, and other employees may engage in fraudulent and other criminal activities. Countries are likely to have their own arrangements for investigating allegations of wrongdoing, which could include fraud against stakeholders and cybercrimes. Such activities might also be undertaken by a contractor or occur within a business, supply chain, or value chain partner.

Special arrangements, entities, and/or units may exist for handling economic crimes, international fraud, and serious fraud cases. They can vary in competence and focus. National companies in certain authoritarian countries are required by law to serve the interests of the state. The integrity and safety of financial systems and whether people and organisations at home and abroad have confidence and trust in them can be especially important for corporate operations and international business development. Protecting them may be a high priority for different entities whose work may also require the support of businesses.

Recognising board responsibilities and corporate exposure

Boards may face certain sensitive decisions relating to cyber security and crime, involving questions of what to acknowledge and report, how to react to ransomware attacks, whether and in what areas to trust, and with whom to collaborate. Difficult choices may sometimes need to be made between what is most beneficial for a company and what might best serve the public good. Directors may err on the side of caution, especially when a local agency may lack the means and motivation to make beneficial use of the information provided.

Boards may be reluctant to acknowledge that a company has been the victim of a hack or a cyber-fraud for fear of alarming those who deal with it and the damage to confidence, trust, and a corporate reputation that might result. By not reporting and describing a breach, law enforcement agencies may be denied information they could use to protect others as bad actors attempt to repeat a successful penetration with other targets. Delays while assessing, discussing, and seeking approvals at each entity in a response chain can expose others to risk.

Directors should consider the possibility and risk of harm caused by weaknesses in an entity's own systems. These could range from captured devices being used to mount cyber-attacks on other people and organisations, through the use of its products and services by bad actors, to direct harm to others caused by its applications of AI and AGI. Appropriate warnings could be provided and steps taken to avoid exposing people and organisations to

unreasonable and unacceptable levels of risk. Liability for damages could be considerable.

Understanding AI and AGI vulnerability and exposure

Criminal gangs and state and non-state proxy actors can themselves use accessible AI and AGI applications to quickly analyse large quantities of data, search for areas of weakness and vulnerability, and endeavour to move before others have updated their protection. In the race to stay up to date and exploit, malevolent actors who are not constrained by lengthy approval processes and may operate 24/7 can be at an advantage. To succeed in their ambitions, they might only need to occasionally penetrate a small number of the systems they monitor.

Some bad actor actions may increase the impact of other malevolent activities or create new opportunities for them. Mass insertion of biases into social media could affect AI applications that are trained with the resulting data. Over time, more of the data used to train AI tools and applications might itself be generated by their earlier generations and use. In time, this might result in the collapse of certain models. Malicious attempts may also be made to poison data. Being unaware of who is using an offering and for what purpose might result in exposure.

An international interim scientific report on the safety of advanced AI ahead of the 2024 AI Seoul Summit has highlighted the wide-ranging potential beneficial use of general-purpose AI, limited understanding of its capabilities and inner-workings, and dangers and uncertainties regarding trajectories of future progress. In addition to malicious use of AI for large-scale disinformation and influence operations, fraud and scams, applications could disadvantage certain categories of people, while future advances could pose systemic risks.

Considering and scoping collaboration

The interim report produced by the UK Department for Science, Innovation, and Technology (DSIT) and the AI Safety Institute reveals differing views among experts about the risk of loss of human control over AI applications leading to catastrophic consequences. Current methods of mitigating risks, including benchmarking, red-teaming, and auditing training data, are considered to have limitations. Improvements are required. Overall, the future seems uncertain, various scenarios are possible, and international collaboration is advocated.

At a global level, geopolitical fracturing is occurring. Collaboration with certain states that actively support, or whose proxies use, malicious applications to attack and undermine democracies and various ways of weaponizing AI, collaboration, and knowledge sharing in certain areas is increasingly problematic. Bad actors have a vested interest in undermining trust in bodies and law enforcement agencies that might benefit from greater candour and knowledge sharing by companies concerning the cyberattacks they are experiencing.

Bad actors can collaborate, as can their targets and victims. The value of collaboration depends upon many factors, including the technical challenge of achieving a breakthrough or 'hit' and what is at stake. Using quantum computing to overcome encryption system defences and expose financial transactions represents more of a challenge than using an accessible AI tool to produce a deep fake impersonation of a person in authority that could be exploited. The development of alternative cryptology solutions should now be a collaboration priority.

> Boards may be reluctant to acknowledge that a company has been the victim of a hack or a cyber-fraud for fear of alarming those who deal with it and the damage to confidence, trust, and a corporate reputation that might result. By not reporting and describing a breach, law enforcement agencies may be denied information they could use to protect others as bad actors attempt to repeat a successful penetration with other targets.

Preparing for possible future scenarios

In some jurisdictions, most companies are either experiencing cyberattacks or are at risk of being attacked. Boards need to understand and discuss the rapidly evolving threats they face, some of which may be state-sponsored and undertaken by malicious actors. They may be well funded, including from the proceeds of cybercrime and/or state support, and more advanced in the applications and methods they use than those to whom a company might turn for advice and support. Obtaining current cyber-security advice is a critical requirement.

Improving protection and decreasing the impact of breaches may require doing things differently. Serious thought may need to be given to reducing connectivity and separating and duplicating important systems, especially critical ones. One should also not assume the continued availability of digital systems or the internet. They could be taken down by natural phenomena or by malicious actions at certain vulnerable points; once bad actors judge, this would benefit them more than further cybercrime and their use to undermine targeted states.

Greater reliance on digital technologies increases the already voracious demand of data centres for electricity and rare minerals required by digital infrastructure. How many companies can operate in an analogue world? Certain existential threats increase the risk of inter-state conflicts, during which one or more state actors may take a hit to their own interests by cutting internet cables to impose greater harm on a target. Prudent boards prepare companies for unwelcome scenarios. They also enhance resilience and back-up arrangements. ■

*__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.