IIMC Library Clipping Service | Source: News: Online: Forbes India | Dated: 17-10-2022

Why cyber-security needs to be a strategy in the infinite corporate game

A typical finite game mindset is harmful in the long run to both, sustainable ROI and shareholder satisfaction, and a robust and secure cyber-space. IIM-Calcutta proposes managerial action items for cyber-security to become an integral part of the business and competition

BY RANJAN PAL, BODHIBRATA NAG AND CHARLES LIGHT

How C-suites in modern businesses handle cyber-risk management will reveal that most of them (90 percent of whom represent SMBs) 'play' the game of increasing ROI against their peer competitors and focus mostly on product/application QoS to woo consumers. Image: Shutterstock

Most enterprise leaders around the globe have converged upon the importance of IoT and CPS technologies (complemented with Cloud and AI) to improve business productivity and consequent ROI. It has become a common strategy across most businesses to compete (akin to a strategic game) with similar peers on popularly established business KPIs via the integration of IoT/CPS technology on the multiple critical business dimensions that include:

1. asset tracking and inventory management,
2. real-time data collection and sharing among business processes on how consumers interact with products,
3. forming new business lines and value-added-services,
4. facilitating Omni channel services,
5. enhancing accessibility, efficiency, and productivity of business processes, and
6. improving customer experience.

Attractive, as it might seem, the benefits of IoT/CPS integration in modern businesses are not without major security drawbacks. When exploited by nation-states and other cyber adversaries, they can majorly disrupt business continuity for up to multiple weeks at the individual and supply chain layers.

A closer look into how C-suites in modern businesses handle cyber-risk management will reveal that most of them (90 percent of whom represent SMBs) 'play' the game of increasing ROI against their peer competitors and focus mostly on product/application QoS to woo consumers. In the process, cyber-security of business processes at various levels of IT/IoT system granularity takes a backseat, even though many SMBs are equipped with necessary resources that can potentially mitigate the cyber-attack space. In this article, we view through a finite and infinite game-theoretic lens the existing glaring issues C-suites of organisations subject themselves to, against achieving robust organisational cyber-security. We argue why a typical finite game mindset prevalent in the business world is harmful in the long run to both, sustainable ROI and shareholder satisfaction, and a robust and secure cyber-space. We also propose managerial (strategic) action items, motivated by the principle of infinite (business) games, for cyber-security to become an integral part of the product/application design process and business competition

Why C-Suites don't make cyber-security a just cause

The main reason why cyber-security breaches affect organisations often, despite being resource-equipped to better manage cyber risk, is that most C-suites adopt a finite mindset and do not promote cyber-security as a just cause. The finiteness is a direct outcome of businesses competing with peers on well-established ROI metrics known to all, and cyber-security does not belong to these metrics. In doing so, businesses become myopic and do not account for the long-term futuristic impact of cyber-security as a new ROI-improving factor. The rationale behind this myopic firm behaviour is based on two main reasons.

1. Historically, according to multiple organisational surveys conducted on CEOs (Source: MIT CAMS), there has been a clear difference between the preferences of the C-suite and the IT managers (e.g., CISOs). The C-suite is

(a) often not knowledgeable and/or passionate about cyber-security,
(b) is sometimes over-confident in their organisation's ability to manage cyber risk and/or the quality of their cyber posture.

In many cases, the C-suites offload the responsibility of cyber-security aspects of the business to the IT wing without making a conscious effort to understand the security loopholes in the business processes and their adverse impact. The one-dimensional fallout of these C-suite issues is that IT-driven businesses do not invest enough in cyber-security as they are (falsely) of the opinion that it does not significantly affect KPIs over time or have an instantaneous impact.

2. C-suites, even those who acknowledge the importance of cyber-security on business continuity, are primarily looking at profit as the main KPI and have their eyes on the external stakeholders and investors. There is hardly a long-term social cause like cyber-security an organisation is affirmative and optimistic about. In other words, the absence of a cyber-security social cause does not inspire a feeling amongst the 'general' employees of being part of a group or great cause advancing cybersecurity and societal well-being, alongside selling attractive products/applications. The major reason here is that application quality and seductiveness often is key to ROI enhancement. These are often anti-security and hence do not inspire profit-minded leaders to pursue product cyber-security enhancement as a major corporate objective that acts as a social cause. The game-theoretic connotation of this point is that business leaders and their employees, usually of finite mindsets, cannot foresee the role of cyber-security in the sustainable increase of business productivity and application attractiveness. Hence, play a myopic game with their peers that do not have cyber-security as a strategy element. On the contrary, it is much more likely that business productivity will be hampered and consumer reach diminished if digitally pervasive business applications and processes are statistically more breachable in a weak IoT security landscape.

3. At the C-suite level, organisations, especially banks, are often sceptical and risk-averse about sharing cyber-vulnerability information with vendors and their partners. They believe that doing so will dampen the consumer base

and cause public outrage—leading to a sharp fall in ROIs. While such negative feelings might hold in the short-term, the strategy of voluntarily revealing cyber-vulnerability information could be a masterstroke in the long run in inculcating a deep-rooted feeling of trust in the consumers. They would be inclined to believe that an organisation is taking steps to inform customers of security loopholes and is continuously trying hard to ramp up its cyber-security posture.

Win-Win Managerial Recommendations Viewed Through the Lens of the Infinite Game

We recommend an expansion of the managerial mindset to account for cyber-security as a strategic variable in business competition. We propose the following recommendations rooted in the concept of infinite games. They will allow organisations to achieve improved business KPI performance, alongside contributing to societal welfare through improved cyber-security emanating from all its business processes and affecting relevant IT/software-driven supply chains.

1. Managers (C-suites) in IT/IoT-driven businesses should not adopt the Milton Friedman philosophy that states that a corporate executive is an employee of the owners of the business. This principle rapidly followed since the 1970s by most of the business world is the root cause behind firms racing towards making profits to solely satisfy their investors—without giving much thought to any just cause or the negative side-effects of the products. If 80 percent of a CEO's pay is based on what the share price is going to do next year, they will do their best to make sure that prices go up, even if the consequences might be harmful to employees, customers, and society in general. In the context of cyber-security,

- an increased push by businesses around the globe to deploy IoT devices with poorly configured cyber-security for improved productivity and efficiency, and
- Google, Facebook, Twitter (and many other ad-driven firms) unfairly selling personal data to advertisers without consumer permission are prime examples of organisations adopting Milton Friedman's principle of doing business.

2. Managers in IT/IoT-driven businesses should adopt an Adam Smith-inspired version of capitalism that is better for society. The management should think of the societal consumer good (social welfare) before thinking of the producer (monetary returns of investors and shareholders). In the context of cyber-security, this means striking a proper balance between quality application features attracting customers and necessary security plug-ins. Such a product design approach should pervade all management, employees, shareholders, and investors concerning business incentive compatibility.

Organisations such as the US Office of Technology Assessment, examining the long-term impact of technology on society, need to be brought back to fashion at least concerning advancing cyber-security of business products and processes. As an example, such organizations should

- check the application features in a product (including open-source code) to see whether important security constructs have been included before they are up for sale in the market, and
- work with auditors and cyber-insurers to ensure a threshold level of cyber-hygiene in organisational employees working on IT business processes.

Moreover, in the context of Adam Smith's philosophy, an infinite-minded leader, to promote their main goal of making cyber-security a just organisational cause, will first realise that the will of people—motivated via an inspiring security-driven organisational motto—will drive its goal through methodical problem solving, imagination, teamwork focussed on the just cause. This leader will be convinced that such an approach will in the long term bring more ROI

and consumer trust to the organisation.

3. The C-suite should avoid the following four market competition pitfalls for the just cause. First, the just cause should not be a moon shot. As an example, in the context of cyber-security, a company should not put forward a long-term goal such as - "we will deploy technological tools such as differential privacy, secure multiparty computation, and homomorphic encryption in our products to protect consumer data". Though this is a strong goal in the security interests of society and should be adopted, it is finite in scope and a moonshot towards a greater idealistic goal of being on the path to continually improving cyber-security. Second, the just cause should not be becoming the best. Egocentric causes often distract the organisation from achieving the social interests of society and bring in too much narrow-minded finiteness to lose out to product competition in the long run. As an example, from a cyber-security viewpoint, an organisation should not promote a goal such as "product with the best cyber-security". In this process, they may be losing out on providing trendy and effective application benefits that the consumer needs. Third, the just cause should not be growth-at-all-costs (unless security is the factor of growth). This mentality, often leading to a tricky space of mergers and acquisitions, is detrimental because there will be inevitable marginal non-security technical improvements in the future for stable products, and it is not always investment-wise (unless the merger is to a security firm, e.g., the Broadcom-Symantec merge) to keep upgrading non-security dimensions without major upgrades on the nascent dimension of cyber-security. Finally, an organisational just cause should not adhere to corporate social responsibility (CSR) for cyber-security. CSR programs should only be part of the broader strategy to advance the cyber-security just cause with the goal being "do good making money" instead of "make money to do good".

4. C-suites should exhibit strong leadership in being worthy rivals in the tech-driven industry competition. For example, in the traditional PC business, Apple had worthy rivals in IBM and Microsoft. If there are organisations in the market that can provide stand-out cyber-security services, others should follow too. This is a special setting, where even a plain imitation of other organizations' finite-minded strategies will do good for society. More so, if there is good market competition for security-promoting tech products, it will be in the positive interest of competing organizations to "outdo" others in terms of market share. On this note, existential flexibility is important for leaders carrying the mindset of being worthy rivals/trendsetters if IT-driven businesses are to advance cyber-security. Leaders must take a risk and flex their minds to realize and envision that security can be as attractive as the main application and motivate the tech minds in the organization to develop solutions that fit this criterion. As an example, the pervasive use of IoT technology in the digital world may be the killer application for cyber-security to be a crowd-puller. To take this risk, organization leaders should have exceptional courage to go against the status quo and enact existential flexibility to

- promote products with strong security, and
- hire a workforce that is willing to invest in improved cyber-security practices within the organisation.

This could imply rejecting the "first to move in the market" mindset and hiring talent that is willing to go the extra mile in ensuring cyber-security best practices through their work behaviour but may not be the best technical mind available for hire.

Ranjan Pal (Massachusetts Institute of Technology, Sloan School of Management) Bodhibrata Nag (Indian Institute of Management Calcutta) Charles Light (Silicon Labs, USA)

Source: https://www.forbesindia.com/article/iim-calcutta/why-cybersecurity-needs-to-be-a-strategy-in-the-infinite-corpo-rate-game/80589/1