Cybersecurity: critical consideration for boards of growth firms

Book or Report Section

Accepted Version

Goyal, Ruchi, Kakabadse, Andrew and Kakabadse, Nada ORCID logoORCID: https://orcid.org/0000-0002-9517-8279
(2021) Cybersecurity: critical consideration for boards of growth firms. In: Poff, Deborah C. (ed.) Encyclopedia of Business and Professional Ethics. Springer, Cham. ISBN 9783319235141 doi: https://doi.org/10.1007/978-3-319-23514-1_1276-1 Available at https://centaur.reading.ac.uk/99885/

Cybersecurity: Critical Consideration for Boards of Growth Firms

Introduction

In contemporary times cybersecurity is a momentous issue. Rapid and expansive digitalisation in the era of the 4.0 Economy, is characterised by inter-connected devices autonomously making 'intelligent' decisions without requiring human intervention. While it has potentially improved decision-making processes, it has simultaneously introduced risk to businesses, in the form of cybersecurity threat. These cyber breaches have a monumental impact on not just the top and bottom line of a company, but also its reputation in the market (affecting its share value), litigation management, as well as customer loss, among other major drawbacks. Thus, many boards are getting involved, even creating executive committees to address this challenge successfully. How do organisations manage such cyber vulnerabilities? Does the answer perhaps lie in cybersecurity governance?

This chapter attempts to answer such questions through developing a clearer understanding of the various aspects involved. Beginning with acknowledging the insightful results of preliminary studies in the field, the characteristics of growth firms and their reliance on stewardship of the governing boards are discussed next. Further, the increasing prevalence of digitalisation through the 4.0 economy is understood to explore the subsequent concerns surrounding cybersecurity. Having thus set the background for cyber issues, the next subsection discusses the prominent issues concerning cybersecurity and an organisation's vulnerabilities it exposes. The solution is then investigated through incorporating cybersecurity as a critical element of an organisation's corporate strategy in the next subsection, before concluding the chapter with closing remarks.

Findings from Preliminary Study

An initial study in this field, supports the view that irrespective of the industry sector a particular organisation may belong to, their product or service offering inextricably encompasses a digital existence. Thus, a firm's concerns related to cyber-realm are not only a preventative choice as an element of their risk compliance, but a real action point owing to the clear and present danger posed by progressive susceptibility to cyber threats. It then contributes to the view that investment of time, finances, and other resources like increased director focus, must understandably be earmarked for cybersecurity.

More so than before, it has become a priority of the boards to allocate adequate resources toward managing the organisations' cyber-risk. Board dynamics with respect to the governing

boards' type of director characteristics, including their background and their tenure in the firm, contribute to the firm's overall response to cyber-vulnerability. In some firms, this involves hiring directors with past experience as technology directors or CEOs of technology firms, in others, it has translated to encouraging members with technological experience/ expertise. Furthermore, instead of prescheduled formal bi-annual or quarterly meetings, boards are attuned to the dynamic and volatile nature of the technological world, and are employing a flexible approach to interacting frequently, including remote virtual meetings.

The overall findings highlight the fact that owing to the combined influence of – the dynamic nature of the field, ever-evolving technological landscape, and the unfathomable motivation of cyber-criminals - it may be infeasible to guarantee a lack of cyber-vulnerability. There cannot be a scenario where an organisation could ensure a lack of cyber-campaigns hurting its reputational, financial, and legal standing. However, a fortified and comprehensive cyber-strategy which evolves with time and is largely reliant on board-preparedness may yet be the answer to safeguard the present and future of growth firms looking to expand and grow. This brings to growth firms and the characteristics which differentiate them from other small and medium sized firms.

Growth Firms and Their Boards

Growth firms have been identified as those with either employment based or productivity based fast growth most prominent with small firms in the first five years of their lives (Du and Bonner, 2017). Such firms abound in all sectors of the economy, including manufacturing, business services, and other service sectors. The interesting point highlighted by studies is that having high/ fast growth firms in a particular sector or industry contributes to subsequent growth for that industry overall (Bos and Stam, 2011). Thus, growth firms are not only beneficial for themselves turning into potential mega-firms of the future, providing employment, boosting the industry sector, they also lead to the development and growth of the economy.

This further highlights the behaviour of growth firms, vis-à-vis their strategic plans for growth, their identification of their competitive advantage, propensity for risky R&D, and innovation challenges. It has been seen that such firms often respond to economic crisis and competition through investments in product innovation and development into international markets. They have been seen to be more amenable to investments in the field of R&D and responding actively to innovation challenges. With time, as the firms grow older their strategic choices may align

more with predictability and lower associated risks. Their strategic choices bear, in turn, largely on their governing boards and the way they envision the firms' future.

Aiming to metamorphose into large conglomerates of the future, growth firms especially rely on their corporate boards to thrive. In such firms, the focus is to bring on board directors with ample access to expertise and other resources, which will reduce their environmental dependency and thereby, future uncertainty. Often, high-technology or other firms with large R&D focus tend to be often resource poor. To resolve this resource impoverishment, the firms specifically rely on the outside board member capital – which encompasses human, social, and financial capital (Clarysse, Knockaert and Lockett, 2007) which would allow the young growth firm with the necessary access to the resources and a potential source of competitive advantage.

In addition to providing access to resources, the stewardship role of governing directors is another prominent feature in governance of growth firms. Besides monitoring the management, providing support, and crafting and drafting the organisational strategy, the board's multi-pronged role as mentors/ stewards is vital for growth firms, as opposed to their larger counterparts. Since such firms rely on technology as a corporate asset – including customer information, employee data, intellectual property, and other elements of their cyber identity – the company development through technological survival becomes an indivisible element of a director's stewardship role.

Another characteristic feature of growth firms is their reliance on their founder for strategic direction that the firm adopts, as well as the possibility of CEO duality. Studies prove the frequent incidences of the firm founder being on the governing board as well a member of the top management team. This has further implications on the board dynamics at play when it comes to strategy making for the firm, including for agenda items such as technology resources and cybersecurity processes. Boards under a strong influence from the firm founder and working in a unified fashion would be far more likely to act fast and with more flexibility for situations arising out of the dynamic nature of issues, as is the case with cybersecurity concerns.

Thus, for identifying its competitive advantage, firms often look either inside the firm or outside the firm in the market. Technological uniqueness may provide the firm, the technology to act as a potential source of competitive advantage to the young entrepreneurial firm. Thus, for a growth firm, the dynamics of the board, and the firm's reliance on technology as a value-creating asset, weigh heavily on its decision to identify its competitive advantage with respect to its future vision for growth. However, the contemporary dynamic of an increasingly

digitalised world adds another layer of complication for the growth firms, which is discussed in the following section.

4.0 Economy of Today

Historically, the above two factors of an organisation's board dynamics and its dependence on technology may have been sufficient to influence its vision and strategy for technology. However, in today's scenario the world of technology itself is far advanced than it has ever been, and it may be expected to evolve consistently. The impact of interconnected devices, autonomously making decisions, not held back by the need for human intervention, are the standards of technology in today's era.

This 4.0 economy has been characterised by jargons of the digitalised world of today – Artificial Intelligence (AI), Cloud Computing (CC), Machine Learning (ML), Internet of Things (IoT). Even for an ordinary firm outside the scope of automated manufacturing, or high-technology industry, the above technologies signify a digitalised world characterised by automation, connectivity, and intelligence (Piccarozzi, Aquilani and Gatti, 2018). In such a context, whether an organisation functions in the technology industry or not, their reliance on technology is higher than ever before. Thus, safeguarding an organisation's complicated cyber-realm is critical in today's 4.0 economy.

Unlike firms of yesteryears, which ordinarily relied on hiring an individual/ team to fulfil the technology requirements of the entire firm, today's firms are characterised by more top-centric strategic focus on technology. Increasingly, technology as an element of strategy dynamic is in the purview of the governing boards, instead of centred in their technology department or the technology member of their executive team. Pre-empting technological concerns and preparing for them with adequate investment, expertise, experience, and insurance is a priority for organisations and their apex bodies. The focus, thus, on these apex bodies/ governing boards is to incorporate technology as a focal point of their strategy.

This is not to exempt the need for the organisation to recognise cyber-concerns as an enterprise-wide risk. However, the perspective has evolved to appreciate involvement of the top of the strategic pyramid – the governing boards – while ensuring, the rest of the firm's participation in cyber-vigilance. Since, many cyber-campaigns target an organisation through its most vulnerable touchpoints (which are often its employees), the onus is on the entire firm to be vigilant against cyber-vulnerabilities. But what are some of these cyber-vulnerabilities and how are they significant issues for growth firms? This is explored in the next section.

Contemporary Issues with Cybersecurity

Cybersecurity as Vulnerability

Cybersecurity as a construct has been relevant since the past few decades, when early mentions of '*cyberwar'* (Arquilla and Ronfeldt, 1997) was enough to provoke a global fear among the academic and intellectual community. However, in the current millennium, it has moved from a fictional to a credible threat status. Organisations are exposed to cyber-vulnerabilities, from malicious campaigns by both state and private actors. Hackers, hacktivists, organised criminals, and states are responsible for cyber-attacks which have had and continue to have calamitous impact on their victims.

Reputational, financial, and legal risks worth billions and sometimes enough to demolish a firm, have made the cyber-realm a potentially dangerous and vulnerable world. Furthermore, being a virtual impossible to protect through usual borders/ boundaries, there challenge to protect and safeguard assets is further complicated and magnified. While large organisations with potential of large losses most often cannot avoid mass attention when such events occur, but this does not mean that smaller sized firms escape such attacks. Traditionally, security threats were less vicious, which could have been natural disasters, theft of hardware/ software, unauthorised access, or human error (Loch et al., 1992). However, in modern times these have become more hostile and targeted, as hacking and cyber terrorism continue to rise.

One way to approach cyberspace attacks could be to first identify the potential point of entry of the threats themselves. Access points to the organisation are often the vulnerabilities targeted by cyber-criminals. These could be through proximity (through a victim's network), through an insider (unwitting players fooled into sharing access), supply-chain (through software/ hardware doors), remote (hacking), or even denial or access (flooding the victim's server incapacitating it). Thus, the burden of maintaining cyber-integrity lies not only on the shoulders of the governing board, but the entire machinery of employees and other stakeholders.

Concerns Arising Out of Cybersecurity Vulnerability

Increasing practitioner reports, academic studies, and policymakers' surveys outline the status of cybersecurity as a focal point in contemporary times. The National Cyber Security Centre, as a unit of the Government Communication Head Quarters, is the UK government's initiative towards ensuring a safe and strong cyber-realm for individuals and organisations alike. Keeping a close eye on the developments in the field it has recently reported an alarming

increase in the incidences of cyber-attacks on organisations (46%). Of these, the majority were from phishing campaigns (86%) in recent times. Subsequently, an increasing number of governing boards (80%) of organisations are realising the need to turn the strategic board spotlight on cybersecurity.

Within the UK alone, an average FTSE 100 firm is expected to have a permanent decline in its share value of about 1.8%, which in financial terms may be translated to about 20million GBP (CGI-Oxford study, 2017). Figures such as these, highlight the severe impact of cybersecurity lapses and incidents on organisations today. Whether the firm operates in the field of technology or not, its reliance on technology for its operational functionality or as a repository of useful company information, renders it susceptible menacing cyber-attacks aftermath. Given that such attacks may very well originate at the hands of an over-eager individual, or an organisation, or even an enemy state magnifies the risks that organisations must come to terms with.

Hackers (individual with potential for cyber-attack) are frequently in the news for having gained illegal access to and with potential towards wreaking havoc. An American teenager recently hacking the social media accounts of Joe Biden and Bill Gates, is a case in point. Similarly, there are increasing incidences of states (intelligence agencies sponsored by the government) accused of sinister attacks on organisations. The recent attack on SolarWinds software in the US in December 2020, likely perpetrated by over 1000 engineers in Russia, and may be considered the largest and most sophisticated attack ever seen. Besides these, there are also the potential dangers from hacktivists (collective groups trying to influence decision-making) and organised criminals (extortionists on the internet), who pose extreme and unparalleled risks for organisations to shield themselves from.

The state governments and policy makers are aware more than ever, of the growing need for cybersecurity awareness, and the need to have policies and bodies in place which ensure prevention of and addressal to cybersecurity concerns. In the US, Security and Exchange Commission (SEC) and the IT Governance Institute have been placed to supervise transactions in the cyberspace. European Union's General Data Protection Regulation (GDPR) (implemented from May 25th, 2018) mandates that companies conduct privacy risk-impact assessments to analyse the risk of data breaches. Closer home, in the UK, the Ministry of Defence has several bodies assigned to this task.

The attacks/ breaches can last anywhere between nanoseconds and years, but losses are considered in four primary categories – confidentiality, integrity, availability, and indirect loss (Finnemore and Hollis, 2016). Subjectively viewing the corresponding costs of these losses, the firms need to build capabilities to develop sustainable defences, rather than merely purchase or employ them. When the defences are of a self-sustaining nature, there is hope for them being adequate when the need arises. Thus, governing boards of growth firms must equip themselves through cyber-preparedness to achieve any tangible safeguards towards cyber-vulnerabilities. Delving further into the strategic aspect of cybersecurity is the next section, where incorporating it as a critical element of strategy offers security to a growth firm.

Cybersecurity as a Critical Element of Strategy

Corporate oversight allows boards to pre-empt the risk associated with cybersecurity and strategize accordingly. For growth firms, this oversight function needs to be more nuanced through a board's stewarding role, outlining a customised evolved process which evaluates and addresses cybersecurity risks and offers solutions effectively. In the absence of absolute certainty (which may never be a feasible reality in this field) and perfect solutions, the above may be the most practically reliable solution available to corporations. This could even be replicated by other policy makers even at a state level.

The governing board along with its executive team has to determine if the competitive advantages are being created from these opportunities, while simultaneously dealing with the risks (Grove and Clouse, 2017). Since business technologies are integral to how businesses operate, boards need to acknowledge the need to prepare for IT as a resource at the board-level, instead of delegating it. As discussed above, firms need to invest in their information or business technologies based on their perception of risks and the value that the technology adds to the firm's business.

Furthermore, in the digitalised world of today, there is an increasing need for organisations to work together with policymakers, in strengthening their cyber-realm. While government and state authorities create policy and take action, organisations ought to incorporate cybersecurity as part of their strategic component (Cunningham and Head, 2019). Just as workplace safety and security measures are part of the business culture, so do efficient cybersecurity practices need to be ingrained in the normal course of business. For organisations, a successful response to cyber vulnerabilities could certainly be an investment worth making for all the reputational, legal, and financial costs it would save.

Conclusion

Governance of cybersecurity does not merely apply to the administration of threats, rather it extends to ensuring a framework in place under which all future potential threats could be readily addressed, with a top-down approach. The board's role as a steward thus encompasses this critical aspect of incorporating cybersecurity governance as part their strategic mindset. For any ordinary firm, these choices will most likely shape the probability of their surviving in the future, while for a growth firm these determine their ability to establish their market dominance thus securing their future.

The first step, then, is for the board to turn the spotlight on cybersecurity as a strategic agenda item. Evaluating and improving organisational resilience to cyber-campaigns, executing cybersecurity strategy is going to be the task of governing boards, as they craft corporate strategy. Having strategically prepared for cyber related eventualities, organisations then need to ensure that measures are adopted by the entire organisation and all the stakeholders involved. For growth firms to be able to continue growing and become the potential *unicorns* of tomorrow, cybersecurity as a critical element of strategy is vital.

References

Arquilla, J. and Ronfeldt, D. (1997) 'CyberWar is Coming', in *Preparing for Conflict in the Information Age*.

Bos, J.W. and Stam, E., 2011. Gazelles, industry growth and structural change. Discussion Paper Series/Tjalling C. Koopmans Research Institute, 11(02).

CGI-Oxford Economics Study (2017). Available at: https://www.cgi.com/sites/default/files/2018-08/cybervalueconnection_full_report_final_lr.pdf (Accessed: 12 March, 2021)

Clarysse, B., Knockaert, M. and Lockett, A. (2007) 'Outside board members in high tech start-ups', *Small Business Economics*, 29(3), pp. 243–259. doi: 10.1007/s11187-006-9033-y.

Cunningham, P. and Head, S. (2019) 'Cybersecurity Readiness as a Business Value', *The RMA Journal*, 101(5), pp. 16–26.

Du, J. and Bonner, K. (2017) 'Fast-growth firms in the UK: definitions and policy implications', *Enterprise Research Centre*, (October), pp. 1–31.

Finnemore, M. and Hollis, D. B. (2016) 'Constructing Norms for Global Cybersecurity', *The*

American Jounal of International Law, 110(3), pp. 425–479.

Grove, H. and Clouse, M. (2017) 'Corporate governance for trillion dollar opportunities', *Corporate Board: role, duties and composition*, 13(3), pp. 19–27. doi: 10.22495/cbv13i3art2.

Loch, K.D., Carr, H.H. and Warkentin, M.E., 1992. Threats to information systems: today's reality, yesterday's understanding. Mis Quarterly, pp.173-186.

Piccarozzi, M., Aquilani, B. and Gatti, C. (2018) 'Industry 4.0 in management studies: A systematic literature review', *Sustainability (Switzerland)*, 10(10), pp. 1–24. doi: 10.3390/su10103821.