

Cyber-incidents: Formidable impediments or paving stones to organisational wisdom?

Ruchi Goyal, ruchi.goyal@henley.ac.uk

Nada Kakabadse, n.kakabadse@henley.ac.uk

Andrew Kakabadse, a.kakabadse@henley.ac.uk

Henley Business School, University of Reading, UK

Abstract

Baiting, phishing (Conteh and Schmick, 2016), spear-phishing (Bullee *et al.*, 2017), and whaling (Pienta, Thatcher and Johnston, 2020), are not leisure time activities; but types of social engineering cyber-attacks (Conteh and Schmick, 2016), which involve tricking a user into either divulging sensitive information or gaining unauthorised access into their systems. However, there are also cases when proactive organisations are able to safeguard their cyber realm against such breaches. At other times, some organisations are fortunate to learn from the cybersecurity mistakes of their peers (Ashraf, 2022).

Since every other day brings news cyber-incidents, perhaps these offer the proverbial steppingstones to wisdom. In the contemporary era of digitalisation, with widespread dependency on complex digital systems (World Economic Forum, 2022), cyber space acquires a vital significance. Drawing on insights from a recent study conducted by the authors, this paper explores this aspect of cyber-incidents of learning valuable lessons from cyber incidents on the path to robust cybersecurity.

Word Count: 5001

Introduction

In this era of digitalisation, a considerable majority of social and professional interconnections occur in the virtual realm. Thus the future arguably belongs to this virtual space (Bejan, 2022) and hence the securing that realm is a vital step in the process of future making as pointed out by Whyte, Comi and Mosca (2022). Within this context, it is impossible to ignore that campaigns against an organisation's information and information systems have been growing in their number, variety and, severity (Fulford and Doherty, 2003).

The retaliation to the Russian invasion of Ukraine by the so called IT Army of Ukraine (Ulea, 2022) - consisting of volunteers - which has hacked through vital Russian websites (including, the Kremlin, the Duma, state-owned media, banks, and energy suppliers), is a case in point of the cyber war previously highlighted by scholars (Arquilla and Ronfeldt, 1997). Other instances are similarly disturbing in nature, and include the 30million customer data breach of the Indian Railways in December 2022 (XTI, 2023), the 5.4million Twitter user records available released consequent to a data breach in November 2022, and the Optus - second largest Australian telco company - data breach in September 2022, are a few instances on the ever-expanding list of recent cyber-attacks.

The damages posed by cybersecurity breaches to an organisation's reputation, financial standing, legal situation, are relatively well known. These are the primary reasons a firm would want to take measures to guard themselves against potential cyber vulnerabilities to their best abilities. However, another area that requires attention is also the relative market loss that the cyber-victim undergoes as rival firms may be able to gain from the former's cyber challenges, even when the cyber-attacks were not facilitated or sponsored by them. Thus, this paper explores the unique perspective of examining cyber incidents and attempting to draw insightful lessons from them. To accomplish this, the study wanted to discover the answer to the research question:

On the road to robust cybersecurity, how can organisations learn from cyber incidents?

Cyber-Incidents: Making Sense of and Learning from them

It is increasingly clear that, while failing to implement basic block and tackling practices has been equated with forgetting to lock the back door (Landefeld, Mejia and Handy, 2015), cybersecurity measures are not a measure of choice anymore. During the recent years, there is not the possibility to have avoided being made aware of a major cyber campaign against an organisation, as it gains immediate and wide public attention and interest. 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 (Lock et al., 1992). However, in contemporary times these have become more hostile and targeted, as hacking and cyber terrorism (Furnell and Warren, 1999) or virus (Post and Kagan, 2000). But the list of potential nefarious cyber activities is not limited to hacking and terrorism.

Understanding Cyber-Incidents

To understand the origin and impact of cyber incidents, the elementary first step comprised of examining the motivation and its types, which cyber incident perpetrators are propelled by. While the reasoning may vary depending on the cyber threat actor/ criminal, scholars have been able to broadly categorise these into five main motivations (Thackray *et al.*, 2016). These are:

- profit or financial motive - which may be considered to be the most frequent factor driving a cybercriminal, who wishes to be able to disproportionately augment his financial resources
- recreation - is another common denominator amongst some cybercriminals, who conduct an attack owing to the associated thrill or intellectual curiosity of the exercise
- revenge - may be considered associated with notions of personal or social justice where an individual or a group wishes to avenge a perceived wrong
- ideology - is the motivation behind nationalist or other state-driven forces justifying the act for their so-called principles
- prestige - may be considered another kind of attack perpetrated arising out of the sheer ability of the criminal, and/ or their sense of pride at being capable of it

Discovering the reasoning behind any criminal act is often a vital step in finding a resolution to an already occurred event or preventing future events of such kind. The next step in appreciating cyberspace attacks may be to identify the potential point of entry of the threats themselves. Since these breaches occur in the cyber realm of the victim's information and communication technologies, there are five potential sources of cyber vulnerabilities commonly used by cyber criminals. These are (Finnemore and Hollis, 2016):

- proximity access – allowing an adversary to connect through to the victim's network or another way enabling a connection
- remote access - hacking, which does not require connected access and can be perpetrated from anywhere across the internet
- insider access – through unwitting players fooled into sharing access or social engineering techniques like spear-phishing (an adversary poses as a trusted party to induce them to introduce malware (eg. through an email attachment) into the system)
- supply-chain access – built within the software or hardware back doors, during creation or servicing
- denial of access – (DDoS – distributed denial of service) essentially flooding the potential victim's website server incapacitating its ability to respond and/ or disabling it for others

The damage from cyber breaches is worth billions in currency, but losses are considered in four primary categories – losses of confidentiality, integrity, availability, and indirect loss (Finnemore and Hollis, 2016). While the attack and the breach can last anywhere between nanoseconds and years, it is estimated that on an average the adversary has access to the system for 205 days before being detected (Mandiant Threat report: M trends 2015: A View From The Frontlines). Such cases bring to light the need to invest in resources which help build competences which are helpful against above mentioned campaigns. There is also a growing need to build capabilities to be able to develop (Kiss, Breda and Muha, 2019) such defences over time, rather than just purchase or employ them. When the defences are of a self-sustaining nature, there is hope for them being adequate when the need arises.

It has been found that the greater the relative importance of IT to the firm's ongoing operations, the greater the risk potential it faces (Parent and Reich, 2009). The elementary question then is – how does it prepare for cybersecurity in a fast-changing environment, where so little is known and threats are novel? The answer lies in taking a top-down approach wherein the focus of deciding and preparing lies with the governing board. It has to approach cybersecurity as part of its risk oversight function, providing effective governance over information technology (Trautman and Alternbaumer-Price, 2011). However, there is no one-size-fits-all scenario for this field where, cybersecurity needs are highly subjective to each firm and therein lies their approach to it.

Cyber Incidents - That which does not kill us, makes us stronger!

“What doesn’t kill me makes me stronger.” - Nietzsche and Levy (Twilight of the Idols, Aphorism number 8, Maxim and Arrows, 1909). This statement derived from the renowned philosopher and scholar may be employed in the context of cybersecurity to learn from cyber-incidents, thus shaping a stronger and safer organisational future. While cyber-incidents may justifiably be viewed as unmitigated disasters, leaning on strategic military (Krasznay and Hámornik, 2019) as a defence perspective would allow learnings to be drawn from them and used to adequately prepare for a cyber-secure future.

Each day organisations are bombarded with hundreds of cyber breach attempts which are rendered unsuccessful owing to sturdy organisational cybersecurity measures. Studies have noted that following quickly resolved smaller incidents, coupled with security upgrades these incidents may also be observed to reduce in severity over time (Kuypers, Maillart and Paté-Cornell, 2016). Such research is encouraging to the field of cybersecurity research, and the otherwise dismal statistics and overall impact of cyber-incidents. It highlights not only the ability to prevail over cyber breach attempts, but also the potential to learn and outmanoeuvre these cyber-incidents in the long term.

For many organisations these cyber-events are witnessed from afar as others in separated by industry or geography suffer from cyber-attacks, and often succumb to them. Drawing insights from the experiences of one’s organisational rivals (Ashraf, 2022) is the metaphorical *gold dust* for organisations to learn from and better equip their own cybersecurity mechanisms. This may also embolden certain firms to otherwise only be motivated to manage the cyber-incidents, instead of proactively prevent them, through robust cyber strategies. However, the growing dependence on digital sphere (World Economic Forum, 2022) and ever-increasing cyber risks are globally recognised and thus drive organisations to prepare accordingly.

Organisations are increasingly employing a top-down approach to governing cyber-risk rather than managing cyber-incidents, which is another promising step to fortifying organisational present and future cyber-defences. With such an increased impetus to advance their cybersecurity, the incidences of cyber-breaches are more manageable for such organisations. Cyber-incidents then further enable them to learn better ways to strengthen their defences, ranging from hiring the most adept personnel (starting at board level downwards), stringent employee training drills (extended to governing board members as well), purchasing cyber insurance, to acquiring evolving cyber certifications.

Theoretical Perspective

There are many novel approaches to the field of cybersecurity, and academically investigating them could be the first step to understanding their possible effectiveness. A valid suggestion so far as to expand the horizons of research into the field, these approaches are certainly worthy of being explored further. An interesting study was carried out to explore the association between the network services a particular computer node is hosting and the threats it is susceptible to. This was done by drawing parallels in the field of epidemiology, by drawing inspiration from tools used in genetics to identify associations between mutations and diseases (Gil, Kott and Barabási, 2014). It is just an example of the kind of academic exploration being made in to the field of cybersecurity, to better assess potential models for finding solutions in algorithms and statistics. The problems of the internet are being sought to be resolved by solutions on the computer.

Scholars have identified the need to address the challenges posed by Industry 4.0, with combined elements of soft skills, dialogue-based techniques (open and explicit risk discussion) (Kaplan and Mikes, 2012), and envisionment (scenario-planning) (Leonhardt and Wiedemann, 2015). This research relies on the foundation provided by Discretionary Leadership Theory (Korac-Kakabadse and Korac-Kakabadse, 1997). This theory also incorporates the need for dialogue-based techniques, even extending it to polylogue or multilogue (Kakabadse and Kakabadse, 2005), within the role and the nature of the leader's role as determined by him. Growing interconnectedness in the digitalised era of 4.0 economy leads to greater innovation in information and communication technologies (ICT), further leads to a networked organisation. Such organisations benefit from discretionary leadership, founded on the leader choosing a sustainable future through co-creating value (Kakabadse and Kakabadse, 2005) with other stakeholders.

Other scholars such as (Sallos *et al.*, 2019) have proposed an approach of applying a strategic lens to the field. This would combine holism with other approaches like pragmatism (pragmatic approach), inference (adequate strategic inference of cybersecurity efforts), and adaptation (calibration based on feedback). They highlighted the need for an approach which is rigorously formulated and continuously adjusted, so as to make it most adequately applicable. Thus, the approach to cybersecurity would be subjectively dependent on the firm it is to be decided for. Cybersecurity for a small retail company as opposed to a large financial enterprise would have varying needs and outlook. However, the need for it to be evolving with time and developing resilience, is vital.

The field of cybersecurity often encompasses the organisation's *duty of care* (Lunn, 2014) within the director's oversight role, which runs parallel to the *sense of care* (Kakabadse and Kakabadse, 2005) for the community, incumbent upon a discretionary leader in the theory. From a leadership position, cybersecurity stance of an organisation may also be decided on a strategic manner, impacting the level of priority it garners, as well as the operational support that lends itself to it. Thus, for an organisation either directly or indirectly affected by a cyber incident, may choose to view such an incident as an obvious negative event, or in a positive perspective with a view to learning from it. This further encapsulates the shifting mindset (Kakabadse and Kakabadse, 2005), the discretionary leadership is able to achieve within an organisation. This study thus relies on the theory, to help comprehend this aspect of cybersecurity and finding improved ways of governing it.

The Study

This research aims to explore the fascinating and increasingly relevant area of cybersecurity and how boards use it as a tool of strategic planning, in the paradigmatically evolved world of technology. Qualitative research inherently views reality as perceptions and actions of the individuals of the society. This study is investigating the cybersecurity and its positioning within boards of directors, and is thus qualitative in nature. This phenomenon cannot be measured in numbers, and can only be comprehended through in-depth conversations with the governance and top management teams of corporates; highly dependent on their subjective understanding of it. This study is completely dependent on how the board members view it and, the authors further interpret it. It follows then, that this research presumes that the reality is constructed by the actor (board members in this case). Hence, this research adopts the ontological - epistemological position that follows from that differentiation – Constructivist- Interpretivist perspective.

Investigational research (Turner, 2010) has many paradigms and interview protocol has foundation in data gathered through the participants, through which the theory is eventually developed. It is most often adopted as part of the interpretative research which presupposes interpretation to be an integral part of researcher's actions (Nielsen, 2007). Thus, interviewee's description of their experiences in a given situation or context provides useful information to appreciate the data with respect to the subject matter. From the perspective of this study, since the concept of cybersecurity has found significance in recent years, there is not a comprehensive body of knowledge that explains how boards position cybersecurity in their

strategy. Especially, coupled with investigating the processes and behaviour of boards involved in deciding how to position cybersecurity, the research topic arouses curiosity to understand this phenomenon, and help contribute towards a framework to explain it. Thus, qualitative in-depth interviews were chosen as the choice of research design for this research.

The structural level of analysis carried out for this study was at the top of the corporate pyramid, which is boardrooms. Hence the level of analysis for this research is the board of directors. By exploring how individual directors approach matters of decision-making related to cybersecurity, this study is aimed at investigating the dynamics and processes of boardrooms. Examining whether cybersecurity is discussed at strategy level or not, informs this study of the degree of significance that bestowed on cybersecurity. In-depth interviews with governing board members and leadership teams throw light on the subject matter. Hence, the unit of analysis is the individual occupying the board director and/ or C-suite executive role. This research investigated how boardroom decisions of cybersecurity strategy come to take place, coupled with the impact of the autonomously connected digitalised world of today on such strategy-making. Thus, a *snapshot* time horizon (Saunders, Lewis and Thornhill, 2009a) was employed in this study.

Strategy related decisions are taken at the top of the corporate pyramid – by the board of directors, in association with other members of the C-suite. Elite interviews addressed the questions related to positioning of cybersecurity within corporates. These were carried out with different types of professionals in different companies – board members, CISO (Chief Information Security Officer), virtual CISO (externally hired Chief Information Security Officer), and other vital members of the C-suite involved in strategic and operational aspects of cybersecurity, chosen through a combination of purposeful and snowball sampling. Further, the entire sample was a cross-section of companies, instead of following one or two sectors to gather the data, thus allowing for heterogeneous sampling to understand key representative themes. Thus, companies under study were from a wide array of sectors ranging from financial services, technology, critical infrastructure (including defence), healthcare to the public sector. These would be in-depth interviews (audio recording wherever permitted by the individual interviewee) with different members of the strategy making team, in different companies, lasting between 30-120 minutes each. Admittance to such a restricted circle of informants, and the process of detailed information collection lasted well over a calendar year.

Working with constructivist leanings, and inductive approach towards theory development, requires an analysis method that allows flexibility of subjectivity. Considering the specifics of the research question, philosophy, methodological approach, and strategy of this study, one approach emerges as the obvious analytical tool of choice – Thematic Analysis. This mode of analysis is often employed to identify, analyse, and report patterns/ themes within data (Braun and Clarke, 2016), which was employed by this research. Cybersecurity positioning as a strategic decision of boards, is an exploratory topic, which relies on exhaustive data collection from board members, to help identify and draw out themes. Furthermore, this study required the researchers to be an active component of the process, which is another trait of thematic analysis approach. It is particularly useful for studies where the themes are abstract, and often identified by the researcher during the process of study (Ryan & Bernard, 2000), which was particularly useful for a topic fast emerging within a dynamic subject area which is ever-changing.

Findings and Discussion

Cybersecurity incidents are one of the biggest challenges that organisations face on their path to creating and executing their cybersecurity governance mechanisms. Many participants pointed out that each day a large organisation faced hundreds or more cyber breach attempts. However, their existing cybersecurity measures ensured that these attempts were not successful in compromising the organisational cyber assets. Without adequate cybersecurity measures, these attempts have the potential to cause compromise, thereby leading to situations of disaster or crisis for the impacted organisation. This study was able to explore the actual scenario of cyber threats and their impact, and brought to fore the following highlights.

Cyber Incidents as Formidable Impediments

Understandably, cyber incidents lead to considerable impact on the reputational, financial and shareholder value losses (Nolan, Lawyer and Dodd, 2019), legal, functional aspects of organisations. But their growing numbers and list of famous victims do testify the significant probability of breaches by every organisation. Many organisations which survive them are rendered unfunctional for extended periods of time, thus making the cyber incidents one of the most significant challenges to maintaining and implementing a robust cybersecurity practice.

Many smaller organisations, or those which are not prioritising cybersecurity are, and sometimes even those who are unfortunately successfully breached by threat actors. The damage to larger organisations is multi-faceted - reputational and financial loss, legal actions

by victims, and loss of customer trust (an indirect risk (Wessels *et al.*, 2021)) - and immediate in their impact. The damage was explained by one of the participants, as following,

“...Because of a cyber-attack or because of something like that the suffrage (damage) is not only in terms of losing customer trust, but also revenue related. Something goes down for a few days or even few hours and the amount of revenue -that a company could lose, it could also be massive.” 22

The attack itself may be intended to have varied impacts, which would then influence the duration and intensity experienced by the organisation which underwent the attack. Scholars have found that amongst the many losses from cyber-attacks, financial losses occur owing to the work stoppages, rather than loss of data itself (Nolan, Lawyer and Dodd, 2019). Another interviewee explained the extent and kind of these damages by giving examples, saying,

“So there are different ways that cyber-attacks can affect an organization. So there's espionage where somebody like a state sponsored actor might be trying to steal, informational secrets from the organization. There is an availability question, so where the organization provides a service and it can be knocked offline by a cyberattack like a ransomware attack. There is a data destruction aspect where you worry about the data being destroyed or getting leaked into an area where it becomes risk from a GDPR perspective. You've got intellectual property theft as well. And then on top of that, you've got just general financial loss. Or you've got reputational risk as well.” 25

Similar sentiments were expressed by another interviewee who hinted at the regulatory (Landefeld *et al.*, 2017) and financial aspects of criminal attacks, when the organisation is required to pay the fines levied by the regulatory authorities, which in itself may pose an additional financial burden on the already impacted organisation. They said,

“Because our customers really do value our service and so loss of reputation is really something that we would find really painful. UM.. directors being taken to court? Yeah, maybe not massively worried about that 'cause we do the right things. A lot of the time (there are) dumb penalties from regulators. Now that is one that should worry everybody. So we're talking about a heavy fine from the ICO.” 21

Scholars have highlighted the seeming inevitability of cybercrime within the cyber realm as the potential of having *barbarians always at the gate* (Trautman, 2014). Furthermore, with increasing motivation and access available to criminal agents, the types, intensity, and impact

of these is ever-changing and perhaps developing in complication with each passing day. It may then be surmised that cyber-attacks thus hold the potential to cause irreparable damage to an organisation. In the very least, these alter the course of the organisational path from that progress and evolution, to one marred by a phase of crisis and its management. However, considering the potential inevitability of these incidents, perhaps there is a way to view them in order to secure the long-term future of the organisation.

Paving Stones for Organisational Future

While we accept the inevitable nature of cyber-incidents, perhaps there is yet reason to hold out hope. Most large and medium-sized organisations face cyber threats - however small - on a daily basis (Kuypers, Maillart and Paté-Cornell, 2016), which they through their cybersecurity defence mechanisms, are able to safeguard themselves from. Similarly many organisations are fortunate to witness a peer/ rival experiencing a cyber breach (Ashraf, 2022), instead of them. Both these kinds of events - whether relatively small, or experienced by others - bring with them the opportunity to learn from them and prepare adequately for the future.

Recent years of cyber incidents have worked miraculously in garnering growing focus on this field from organisational rivals and peers (Ashraf, 2022), who want to avoid similar damage. In cases where the damage can be pre-empted, is even supported by academic research in the realm, supporting the preparedness to cyber breaches as a mechanism that may be relied upon. Sallos et al., (2019) pointed out that if occurrence and consequences of the breach can be understood in advance, then the organisation may be able to adapt to the breach's destructive potential.

“And when somebody else gets breached, you know whilst we have that empathy for our peers, we also need to take advantage. And a breach that somebody else suffers is almost gold dust because it gives you an opportunity to look into your systems and the people you're working with, systems and see what they're doing. And quite often, if somebody gets breached and you look at your systems and you find you're using the same and you're vulnerable, very quickly the investment comes forward because your organization, or the organization working for, doesn't want to be the next headline, so that that makes a difference.” 8

Understandably in the course of running the business, any incident big or small, would lead to damages, but very often an organisation is forced to re-evaluate its cyber mechanisms and measures (Wessels et al., 2021) overall cybersecurity stance and its robustness in preventing

future attacks. Another participant mirrored these sentiments citing infamous incidents as learning, saying,

“I mean, obviously there's lots of lessons we can learn from everything from the Maersk compromise all the way through to WannaCry in the NHS.” 27

One of the biggest learnings that seemed to emerge from organisations which either survived cyber incidents or learnt from observing their peers (Ashraf, 2022), was the inevitability of cyber incidents. One of them articulated it by saying,

“When SolarWinds and FireEye, some of these enormous companies who in themselves - their whole product range is to prevent data loss for clients - and then they get breached, it just demonstrates that nobody is immune. And it demonstrates that all of the basic controls are just so important. The way that the perpetrators got into SolarWinds, and I think the SolarWinds breach was largely picked up by FireEye - a customer of SolarWinds - when they found their systems/ their tools have been breached. So it does demonstrate that even some of these massive global organizations are susceptible.” 8

These findings bring to fore the realisation, that even the worst of attacks have the potential to learn from and equip themselves more appropriately for the future. In certain cases, the organisations have been iconic in their management of the cyber-attack, and earned a favourable reputation (Andrew Carcano, 2019). In others, they have fortified their cybersecurity systems, to prevent and safeguard from potentially more gruesome cyber-attacks. In this era of digitalisation, where the cyber realm is substantial component of human activity and focus, ensuring security and safety in it can potentially bring with unique advantages over their competitors. In the very least, these cyber-incidents can potentially shape a brighter future for the organisation, if adequate lessons have been learned.

Conclusion

Organisations are constantly facing competition, not only from other firms but increasingly in the form of survival. Since cyber space constitutes a considerable component of most organisations' identity, safeguarding it poses an enormous challenge. The threat of exposed vulnerabilities in the cyber realm can force organisations to succumb to an uncertain fate. Furthermore, competition in the market ensures that as one firm loses, another gains. And this is why, the objectives of cyber-attacks may not always be known. Any or all of information gaining, destructive, or obstructive activities (Kiss, Breda and Muha, 2019) could be the goal behind cyber campaigns carried out by state or private actors.

Perhaps the most worrying aspect of cyber breaches is their ability to replicate virtual guerrilla warfare – a single individual could have the capability to invade the resources of an entire organisation, debilitating its system, and paralysing its processes for a variable amount of time. Furthermore, these hostile campaigns are gradually learning from past instances and developing into more malicious and detrimental attacks, worsening the potential damage and recovery possibilities each time. In this scenario, it is of utmost significance to learn new ways to not only manage these cyber-attacks but also use them as levers to equip themselves for a safer cyber space, and a secure organisational future.

Contribution

This study serves as a real world implementation of Discretionary Leadership Theory (Korac-Kakabadse and Korac-Kakabadse, 1997) and expands its context in the cyber realm. It also lends support to the need for a discretionary leader and the opportune position they are in to offer best practices for governing and managing cyber incidents of any nature. This study also contributes to the growing research offering valuable insights to practitioners in the context of business continuity planning, governance of cyber risk, and protecting shareholder interests. Finally, this research helps reinforce the importance of bringing a strategic lens to managing cybersecurity, which may be helpful to authorities supporting and protecting the cyber realm.

Limitation and Future research

Cybersecurity and incidents of the kind are still relatively new and continuously being sought to be understood by experts. Hence, the research runs parallel and is relatively scarce and in the process of development. This study, similar to any other inductive study, may have limited generalisability of findings, as though the interviewees comprised of individuals representing diverse industries and sectors, their results may not be generalised to each of them.

This research is recent and been conducted through the periods during and immediately after the periods of pandemic, and a comparative study in a wholly different time-period may help draw insightful understanding of temporal comparisons. Future research may also explore the aspects examined in this study through a quantitative lens, which would lead to a comprehensive understanding of the field. Furthermore, exploration of the relationship between regulations and cyber incidents, and that between cyber education and skills gap in the cybersecurity industry, may also lead to greater understanding of this dynamic and constantly developing field. Finally, public sector often disregarded in research, yet frequently

victim of cyber incidents may provide useful information regarding critical functions impacting a multitude of people, thus may be another avenue for future research.

References

Andrea Carcano (2019) 'Maintaining a good reputation even when under attack', *Aluminium International Today*. Available at: www.aluminiumtoday.com.

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

Ashraf, M. (2022) 'The Role of Peer Events in Corporate Governance: Evidence from Data Breaches', *Accounting Review*, 97(1), pp. 1–24. Available at: <https://doi.org/10.2308/TAR-2019-1033>.

Bejan, F. (2022) 'Cybersecurity and Cybercrime: Challenges of an Invisible Space', *Perspective of Law and Public Administration*, 11(1).

Braun, V. and Clarke, V. (2016) '(Mis)conceptualising themes , thematic analysis, and other problems with Fugard and Potts ' sample-size tool for thematic analysis', *International Journal of Social Research Methodology*, 5579(2015), pp. 1–5. Available at: <https://doi.org/10.1080/13645579.2016.1195588>.

Bullee, J.W. *et al.* (2017) 'Spear phishing in organisations explained', *Information and Computer Security*, 25(5), pp. 593–613. Available at: <https://doi.org/10.1108/ICS-03-2017-0009>.

Conteh, N.Y. and Schmick, P.J. (2016) 'Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks', *International Journal of Advanced Computer Research*, 6(23), pp. 31–38. Available at: <https://doi.org/10.19101/ijacr.2016.623006>.

Finnemore, M. and Hollis, D.B. (2016) 'Constructing Norms for Global Cybersecurity', *The American Journal of International Law*, 110(3), pp. 425–479.

Fulford, H. and Doherty, N.F. (2003) 'The application of information security policies in large UK-based organizations: An exploratory investigation', *Information Management and Computer Security*, 11(2–3), pp. 106–114. Available at: <https://doi.org/10.1108/09685220310480381>.

Gil, S., Kott, A. and Barabási, A.L. (2014) 'A genetic epidemiology approach to cybersecurity', *Scientific Reports*, 4, pp. 1–8. Available at: <https://doi.org/10.1038/srep05659>.

Kakabadse, N. and Kakabadse, A. (2005) 'Leadership and the Art of Discretion', *Business Strategy Review*, pp. 59–64.

Kiss, M., Breda, G. and Muha, L. (2019) 'Information security aspects of Industry 4.0', *Procedia Manufacturing*, 32, pp. 848–855. Available at: <https://doi.org/10.1016/j.promfg.2019.02.293>.

Korac-Kakabadse, A. and Korac-Kakabadse, N. (1997) 'Best practice in the Australian Public Service (APS): an examination of discretionary leadership', *Journal of Managerial Psychology*, 12(7), pp. 432–491. Available at: <http://www.mcb>.

Krasznay, C. and Hámornik, B.P. (2019) 'Human factors approach to cybersecurity teamwork – the military perspective', *Advances in Military Technology*, 14(2), pp. 291–305. Available at: <https://doi.org/10.3849/aimt.01296>.

Kuypers, M.A., Maillart, T. and Paté-Cornell, E. (2016) 'An Empirical Analysis of Cyber Security Incidents at a Large Organization', *Department of Management Science and Engineering* [Preprint]. Available at: <https://www.us-cert.gov/incident-notification-guidelines>.

Landefeld, B.S.M., Mejia, L.R. and Handy, A.C. (2015) 'Board Tools for Oversight of Cybersecurity Risk', *The Corporate Governance Advisor*, 23(3), pp. 1–9.

Landefeld, S. *et al.* (2017) 'Is_That_a_Target_on_Your_Back', *Corporate Governance Advisor*, 25(6).

Leonhardt, F. and Wiedemann, A. (2015) 'Realigning Risk Management in the Light of Industry 4.0', *SSRN Electronic Journal*, pp. 1–22. Available at: <https://doi.org/10.2139/ssrn.2678947>.

Lunn, B. (2014) *Strengthened Director Duties of Care for Cybersecurity Oversight Evolving Expectations of Existing Legal Doctrine*, Source: *Journal of Law & Cyber Warfare*. Available at: <https://about.jstor.org/terms>.

Nietzsche, F. and Levy, O., 1909. *The twilight of the idols* (Vol. 17, p. 88). Allen & Unwin.

Nolan, C., Lawyer, G. and Dodd, R.M. (2019) 'Cybersecurity: today's most pressing governance issue', *Journal of Cyber Policy*, 4(3), pp. 425–441. Available at: <https://doi.org/10.1080/23738871.2019.1673458>.

Parent, M. and Reich, B.H. (2009) 'Governing Information Technology Risk', *California Management Review*, 51(3), pp. 134–152.

Pienta, D., Thatcher, J.B. and Johnston, A. (2020) 'Protecting a whale in a sea of phish', *Journal of Information Technology*, 35(3), pp. 214–231. Available at: <https://doi.org/10.1177/0268396220918594>.

Sallos, M.P. *et al.* (2019) 'Strategy and organisational cybersecurity: a knowledge-problem perspective', *Journal of Intellectual Capital*, 20(4), pp. 581–597. Available at: <https://doi.org/10.1108/JIC-03-2019-0041>.

Thackray, H. *et al.* (2016) 'Social psychology: An under-used tool in cybersecurity', in *Proceedings of the 30th International BCS Human Computer Interaction Conference, HCI 2016*. BCS Learning and Development Ltd. Available at: <https://doi.org/10.14236/ewic/HCI2016.64>.

Trautman, L.J. (2014) 'Managing Cyberthreat', *SSRN Electronic Journal*, 33(2). Available at: <https://doi.org/10.2139/ssrn.2534119>.

Trautman, L.J. and Alternbaumer-Price, K. (2011) 'The Board's Responsibility for Information Technology Governance', *John Marshall Journal of Computer & Information Law*, pp. 313–342.

Wessels, M. *et al.* (2021) 'Understanding incentives for cybersecurity investments: Development and application of a typology', *Digital Business*, 1(2), p. 100014. Available at: <https://doi.org/10.1016/j.digbus.2021.100014>.

Whyte, J., Comi, A. and Mosca, L. (2022) 'Making futures that matter: Future making, online working and organizing remotely', *Organization Theory*, 3(1), p. 263178772110691. Available at: <https://doi.org/10.1177/26317877211069138>.

World Economic Forum (2022) *The Global Risks Report 2022*. World Economic Forum.

XTI, S.O.C.R. (2023) Major cyber attacks in review: December 2022 - socradar, SOCRadar® Cyber Intelligence Inc. SOCRadar® Cyber Intelligence Inc. Available at:

<https://socradar.io/major-cyber-attacks-in-review-december-2022/> (Accessed: January 7, 2023).