Organizational Architecture, Resilience and Cyber-attacks

Dr Gloria Appiah - Kent Business School - University of Kent

Prof. Joseph Amankwah-Amoah - Kent Business School, University of Kent

Dr. Yu-Lun Liu, National Taipei University of Technology

Abstract–This study develops a unique model of organizational resilience architecture with an emphasis on the ways in which organizations respond to cyber-attacks. The model elucidates the dynamics and approaches through which organizations mobilize and utilize expertise and resources to combat the effects of cyber-attacks on normal business operations. Drawing on recent cases of cyber-attacks against organizations, the study identifies a host of strategic and tactical responses victims used to aid recovery and return to daily activities. The responses are grouped into three stages to demonstrate the steps that organizations can take to enhance their resilience: Stage 1 focuses on proactive environmental scanning and locating potential threats and attacks, Stage 2 emphasizes neutralizing threats and attacks, and Stage 3 focuses on re-designing, upgrading and updating human, technological and financial resources. On this basis, the study sheds light on levels of organizational resilience and strategies for organizational design in withstanding cyber-attacks and security breaches. The theoretical and practical implications of these findings are discussed.

Managerial Relevance Statement–It is increasingly becoming clear that no 21st century business can survive without technology fueling some, or all, of its operations. While this points to an incredibly exciting era, the pervasiveness of technology, has also made organizations vulnerable to vicious cyber-attacks. The 12 months prior to March 2018 alone saw 53,000 reported cases of such attacks across 63 countries. Organizations are clearly not oblivious of the imminent threat and consequences that cyber-attacks pose to them. However, for most, this awareness breeds panic due to a lack of knowledge on which responses are effective for successfully managing threats and attacks. In this paper, we propose a simple model which organizations can seamlessly incorporate to fight against cyber-attacks. We realize from victim stories that it is impossible to completely prevent cyber-attacks, thus, our model is not aimed at making organizations completely protected. Instead, based on previous research pointing to the relevance of recovery efforts, we have drawn on lessons from victims to suggest simple ways organizations can identify sources of threats and recover quickly from the effects of attacks.

Index Terms–cyber-attacks, organizational resilience, decision making, organizations.

I. INTRODUCTION

Fueled by technological breakthroughs, liberalization and deregulations, the world as we know it has become progressively borderless. In parallel, there has been a boom in the use of media and technology in most, if not all, spheres of human activity. Together, these changes have opened organizations up to unwarranted external parties and made them vulnerable to vicious attacks. Indeed, threats from the external environment have surged in the 21st century, with cyber-attacks becoming a regular experience of many organizations [1]. Cyber-attacks are deliberate attempts by an individual or organization to paralyze the information systems of another organization; the acts are aimed at compromising 'the confidentiality, integrity and availability of data' [2, p. 25]. Such attacks, also referred to as digital terrorisms, cyber-crimes and cyber-terrorisms, have dire consequences for affected organizations, including loss of productive days, service disruptions, huge costs towards recovery of systems, humongous legal fines to compensate individuals whose data have been compromised and huge dents in brand image [3]. As expected, firms of all sizes and configurations, have become more attentive to cyber threats [4]–[7] and are increasingly seeking to develop more proactive and robust routines and processes to improve their chances of survival when attackers strike.

Yet, lacking in current research is an examination of how organizations move on from mere reactive responses to developing resilience. In fact, in spite of the upward body of work on cyber-attacks and their effects on organizations [5], we still lack a solid understanding of how organizations can orchestrate resources and expertise to successfully respond to such attacks. Research indications from various fields in strategic management point to resilience as a key attribute organizations can use to deal with environmental upheavals [8]–[10]. Organizational resilience manifests in various ways and may include efforts towards scouting internal and external environments for possible threats, demonstrating abilities to avoid, or recover from shocks of attacks, and flexibility in operations [11]. Depending on the nature of threat and the kind of organization affected, a combination of responses in

relation to these abilities can ensure survival and a total recovery from many high-impact, yet unanticipated risks [12]. Existing studies indicate that enhanced organizational resilience in the face of crises is crucial for wider communities, even beyond the organizations involved. This is because, reduced interruptions to operations during crises ensure quick recovery of the routines and processes of connected businesses and in turn, continuance of normal lifestyles within societies [13]. According to Liu, et al. [14, p. 401], organizational architecture broadly denotes, the 'clear task-to-organization unit mapping in an organizational hierarchy that makes tasks interdependent within and independent between organizational units'. It is also an adaptable outline of the 'workings of organizations', including how resources and activities are coordinated for effective decision making [15].

In the current digital era, appropriating resilience to survive the increasing spate of cybercrimes against organizations is indispensable. The reliance on digital devices within organizations and across supply chains has come with a parallel increase in unscrupulous activities that infiltrate, compromise and often render digital devices and the information they hold, inaccessible. Of the many organizational responses, the ability to 'continuously deliver intended outcomes' during attacks [16], [17] could be the most important for long term survival. Nevertheless, existing literature is yet to systematically consider the ways in which organizations can achieve the resilience needed for the much-needed business recovery and continuity. Against this backdrop, this study proposes an organizational resilience architecture that expounds the ways in which businesses can leverage resources and expertise to respond to cyber-attacks. Based on insights from relevant literature a conceptual model of organizational resilience architecture is developed (see Fig. 1). We use illustrative cases from twenty-one organizations to shed light on the model and suggest ways by which organizations can benefit from lessons learnt by victim organisations.

Our study makes key contributions to research on resilience and cyber-attacks. Firstly, we integrate insights from organizational resilience studies [18], [19] to develop an organizational model

against cyber-attacks. For resilience-related decisions in particular, an organisational architecture elucidates how organizations can develop the processes and routines needed to become more robust in an era of increasing upheavals. Secondly, while organizational resilience is considered crucial for organizations facing all sorts of crises, a recent review of influential studies on the topic in business and management research, found that in terms of contexts, attention had mostly been paid to accident and disasters [20]. None of the influential studies reviewed had been done in the specific context of cyber systems. This is surprising given that complexities and uncertainties surrounding cyber-attacks such as their ability to fester in cyber systems for years without the awareness of victim organizations, present a unique form of adversity, whose study could introduce fresh insights to current knowledge on organizational resilient responses. This study draws on illustrations from a wide range of organizations to contribute to efforts towards building a resilience literature relevant for cyber adversities. In addition, our paper's focus on cyber-attacks, an adversity which is difficult to avoid [21], and corresponding alignment with definitions of resilience as ensuring business continuity during adversities [22], allow for a more realistic and relevant operationalization of the concept of resilience in organizations. Thirdly, inter-organizational comparisons are a pivotal component of competitive organizations. In line with this, our study, which pulls together lessons from previous incidents across various organizations present a potent resource to support future organizations in enhancing their own resilience [23]. In particular, our study equips organizational leaders with up-to-date expertise and superior intellect to make decisions, which are able to enrich their organizations' responses to cyber-attacks.

The paper begins by providing a brief overview of the organizational resilient literature. On the basis of the review, we developed a conceptual model. This is followed by using cases of organizations affected by cyber-attacks to illustrate the features of our model. The final section presents the discussion, implications and future research flowing from the findings.

II. ORGANIZATIONAL RESILIENCE ARCHITECTURE: A CONCEOTUAL MODEL

A. Resilience and cyber-attacks

A cyber-attack is any type of offensive maneuvering that targets information systems, infrastructures, computer networks, or personal IT devices. It is often aimed at gaining control of these systems and compromising their confidentiality, integrity and availability [24]. Uma and Padmavathi [25] grouped cyber-attacks into five categories, falling under the attackers' intent, severity of involvement, scope of the attack, network type and legal classifications. Ghadge et al. [26] found that cyber risks could be grouped according to physical threats, breakdowns, indirect attacks, direct attacks and insider threats. As a result of the highly specialized nature of cyber systems and associated attacks, the bulk of current research on management strategies, is understandably technical, focusing on computing algorithm developments [27], developing new analytical techniques for performing vulnerability analysis, or stating estimations when an attack involves false data injection on information systems [28], [29].

In strategic management circles, few suggestions have emerged on measures to manage cyber-attacks, mostly in supply chain research. Here, Ghadge et al. [26], in their recent review found that researchers mostly focus on management strategies in the pre-attack phase. This involves technical (e.g. password protection and firewalls) and human measures (e.g. security awareness and commitment) aimed at warding off attackers or increasing early human/employee interventions to stall attacks. Other measures are in the form of using distributed blockchain-based data to protect modern power systems against cyber-attacks [30]. However, examples from victim organizations suggest that while this stage could be useful for spotting threats, no amount of preparation is enough to make organizations completely immune to cyber-attacks [21]. The Singaporean Minister of Health, for instance, in response to measures the ministry had put in place after an attack on SingHealth commented

'We *will do our utmost to secure our IT systems. 'However, unfortunately, we cannot completely eliminate the risk of another cybersecurity attack'* (Minister of Health, SingHealth, 2018). In fact, the illusion of safety that come with such protections could make organizations complacent, and often unaware of attacks on their systems until long after it has started [23], [31]. Thus, in the pre-attack phase, organizations would benefit more from organizing themselves in anticipation or preparation for (rather than avoidance of) a possible attack.

There is also a clear need for more research attention on how organizations can manage their activities in the trans-attack (during) and post-attack (after) stages to manage and ensure business continuity [26]. Few studies from relevant fields have offered some suggestions. For instance, Van Hardevald et al. [32] pay attention to identifying potential pitfalls in the activities of carders (a group of cyber criminals who target credit card information), which may signal appropriate routes for security personnel to track down and apprehend them. Others, relying on the theory of attribution offer ways to identify the origin of attacks as part of efforts to contain them [33]. Other responses include the need to document all stages of the attack and tap into insurance covers [34], [35]. In advancing knowledge on positive organizational responses, Sheppard et al. [31] proposed a Cyber First AID plan, which requires organizations to have *adaptable* plans that are able to be configured in response to the unpredictable nature of cyberattacks, ensure that efforts to manage attacks are *integrated* throughout the organization, and *deliberate* at regularly reviewing plans, practices and clarity of individual roles.

At the centerpiece of premier competitive organizations, strategic resilience has gained increased attention from scholars in strategy and operations management [36]. Organizational resilience has sometimes been defined as a firms' ability to proactively scan their environment, identify looming and evolving threats, institute contingency measures to tackle known threats, and prepare for unknowns [36], [37], [38]. Resilience can also be construed as 'the capacity to adapt existing resources and skills to new situations and operating conditions' [13, p. 21]. Other definitions of the concept focus

on capabilities and practices that allow recovery by an individual or organization to a previously stable and functioning state, following an adversity [20], [38]. In line with the latter, resilience can be conceptualized as a core strength that organizations demonstrate, to mitigate and reduce the impact of crises, including natural disasters, industrial accidents, global economic downturns and product failures. Unfortunately, this latter, and more holistic conception of resilience is not often coupled with research in crises management. As Williams et al. [40] note, resilient actors are assumed to escape or avoid crises. In addition, the focus of most studies, as Linnenluecke [20] documents in a review of influential papers on resilience in business and management, have been on organizational responses in the context of accidents, disasters, organizational behavior or supply chains.

Given the complexity, unpredictable and rapidly cascading nature of risks that cyber-attacks present, traditional approaches to fortifying cyber systems against attacks may not bear needed results. This makes organizational resilience – the ability to ensure business continuity in the face of attacks – an important management strategy. According to [22], this understanding of resilience, proactively built into organizational processes can be a distinct source of competitive advantage businesses which survive attacks wield over counterparts who do not. Linkov and Kott [21], use the example of biological systems to explain the centrality of organizational resilience for managing cyberattacks. As biological systems build their immunity over time to adapt and bounce back when attacked by infections, so too must cyber systems and the organizations in which they operate develop immunities, in the form of resilience, not just to adapt, but also recover from attacks. In this study, we recognize the incredible need for this understanding and implementation of resilience within organizations. We, thus, adopt a similar definition to that of Linkov and Kott [21], of what has now become known as cyber resilience, considering it as firms' practices and responses that enable anticipation, recovery, absorption and/or overcoming setbacks induced by cyber adversities. However, we are reluctant to adopt the term cyber resilience strictly for our study, as resilient practices and responses to managing cyber-attacks are

inevitably linked to and affected by resilience in other organizational processes. We consider organizational resilience for managing cyber-attacks a more appropriate conceptualization of the central focus of our paper.

An area of relevant research interest relates to how organizations can enhance their resilience. First, organizations may adopt and embed new and innovative business models [41], [42], [43]. This often require taking a holistic approach to reconfiguring organizations to be able to bounce back after disruptions to their processes, systems, routines or overall business strategy. Some organizations may even institutionalize these models into an architecture, which can be adapted to confront impending or actualized threats [42]. Second, as Crichton et al. [23] indicate, organizations do not necessarily have to go through disruptions themselves to build their resilience. Instead, there are a wealth of lessons to be learnt from counterparts that have been victims to different catastrophes. While contexts and nature of attacks may differ, the authors note underlying similarities in elements of previous incidents in different years, which offer common lessons that could have lessened the impact of current attacks. Examples of lessons could be ways to prevent catastrophic hazards in sensitive industries to appropriate ways managers can communicate updates with multiple stakeholders. Third, the available literature documents the potential positive effects on firms' ability to overcome environmental threats via leveraging internal and external resources, such as expertise and funding. External expertise and resources can be built by deliberately collaborating with relevant networks [28], and forging alliances that are relevant for enhancing resilience [44].

Internally, firms should ensure they have financial reserves to rely on during crises. This is essential to avoid resorting to layoffs, a response which often undermines key social relationships and erodes trust among organizational members, making recovery efforts difficult or impossible [45]. They should also be able to attract and retain top talents and translate such intellectual capabilities into improved performance relating to responses to threats [11]. In other words, accumulation of relevant

human capital, which involves harnessing top talents is one way for organizations to counteract and respond to cyber-attacks. The organizational learning literature offers a pathway to explain this. Organizations broadly learn when employees are able to mobilize and utilize internal and external information to inform decisions, routines and processes [46]. This means possession of up-to-date knowledge and insights is essential in seeking to develop market advantages induced by resilience. It is worth noting, however, that to improve speed and rate of recovery and business function during cyber-attacks, training and upgrading employees would be useful for all employees across departments, regardless of their expertise in cyber systems.

According to [47], the two key enablers of enterprise resilience are: (1) the capability of an enterprise to connect systems, people, processes and information in a way that taps into a synergy of responses to the dynamics of its environment, stakeholders and competitors. This requires inter- and intra-level interoperability and integration within the extended enterprise and (2) the alignment of information technology with business goals, which requires modelling of the underlying technology infrastructure and creation of a consolidated view of and access to, all available resources in the extended enterprises that can be attained by a well-defined enterprise architecture. In line with this approach, Rajesh [48] identified eleven major technological capabilities for resilience in supply chains including capabilities to modify SC design, capabilities of supply flexibility, capabilities of capacity enhancements, level of standardization, agile capabilities, collaborative capabilities, postponement capabilities, inventory capabilities, product rollover capabilities, pricing capabilities and planning capabilities. Enhancements of these capabilities according to [48] augments flexibilities while also increasing capabilities of resilience in supply chains.

Finally, and in one of the most important research advances on crises management in general [49], and cyber-attacks in particular [50] have noted the importance for timely measures to ensure continuance of business activities when crises strike. Such timely responses, which align with

expectations of resilient organizations should be activated immediately crises factors are determined to neutralize and contain problems. At this stage, organizations should be able to tap into relational and cognitive resources that ensure business functions adjust positively to disruptions [51]. This is often indispensable for the organization to remain operational and to prevent liquidation. A summary of some key studies on resilience is presented in Table 1.

The studies discussed so far have suggested how organizational resilience may be particularly useful for successful management of cyber-attacks and signaled some ways of enhancing such resilience. The literature also points to a preference for considering resilience as ways to ensure business continuity during adversities [20], conceptions which we have aligned our study with. According to [21], however, the science or 'methods' of resilience are to be prioritized over the metaphors or 'concepts', which has till date been the focus of organizational resilience research. Indeed, due to its high-magnitude and increasingly current nature, practical representations of organizational resilience in the context of cyber-attacks are urgently needed.

Such practical organizational responses to threats by organizations may be limited by incorrect search of relevant causes of actions [52]. Building on key insights from the reviews above, we propose an organizational resilience model that could help ensure continued business function when confronted with cyber-attacks. Our proposed model, as demonstrated in Fig. 1 elucidates three stages: Stage 1: Proactive environmental scanning and locating potential threats and attacks, Stage 2: Neutralizing threats and attacks, and Stage 3: Re-designing, upgrading and updating human, technological and financial resources. To elaborate the stages in more detail, we utilize illustrative cases and highlight common activities that were done to spot and respond to current and future possible attacks.

TABLE I
SUMMARY OF SOME KEY STUDIES ON RESILIENCE

Studies	Methods	Key Findings
[47]	Literature Review, Position Paper	The study takes the view of enterprises as extended systems and focuses on a framework that identifies attributes of resilience in such enterprises. The findings reveal that the capability of an enterprise to connect systems, people, processes and information in a way that allows enterprises to become more connected and responsive to the dynamics of its environment, stakeholders and competitors. Further, a business is suggested to decrease vulnerability, increase flexibility, adaptability and agility for the extended enterprise.
[36]	Literature Review, Position Paper	This study develops an understanding of how organizations can build capacity for resilience (such as specific cognitive abilities, behavioral characteristics and contextual conditions) through strategic Human Resource Management. The findings propose that a company should equip core employees and units to achieve desired contributions to resilience through their actions when establishing HR policies and practices. Combining the individual contributions through the process of a two-way interaction and attraction-selection-attrition will ensure further effective capacity for resilience.
[53]	Literature Review	This study proposes that Collaborative Networks (CNs) play an important facilitating role in enhancing resilience. Two main classes of CNs have been identified: breeding environments or strategic alliances focused on preparedness for collaboration and goal-oriented networks. The findings suggest that CNs collaborations are not only to support businesses survive, but also be a source of knowledge and new opportunities in uncertain contexts.
[48]	A relational analysis using Total Interpretive Structural Modelling (TISM) and a case evaluation approach are used to demonstrate the major technological capabilities of firms that influence resilient capabilities of supply chains.	To achieve resilience in supply chains, this study identifies 11 technological capabilities, including capability to modify SC design, capability of supply flexibilities, capability of capacity enhancements, inventory capabilities, product rollover capabilities, postponement capabilities, level of standardization, agile capabilities, collaborative capabilities, pricing capabilities and planning capabilities. Enhancement of these capabilities supplements flexibilities while also increasing capabilities of resilience in supply chains.
[23]	Empirical based on official information of seven major incidents	This research proposes that organizations can enhance their resilience by learning lessons from past incidents – including those occurring in different contexts. The authors identify recurring themes/lessons from 7 incidents of different parameters and locations that can be applied across sectors. Examples of lessons include emphasizing the process of emergency processes, training responders in non-technical skills and communicating with the public.
[20]	A review of influential publications	This study indicates that resilience is considered as strengths, perseverance, and recovery capabilities that organizations and employees demonstrate when encountering adversity. The findings reveal that conceptualizations of resilience differ across research streams. In addition, conceptual similarities and differences among these streams as well as insights that can be generalized to other contexts are yet to be explored, and third, few empirical insights for detecting resilience to future adversity (or the absence thereof). Possible areas of future research are the context of resilience organizing for resilience, measuring resilience and multi-level and cross-disciplinary work.
[38]	Qualitative Multiple Case-Study	The research investigates three organizations that had experienced disruptions to examine their processes of response at the onset of disruptions and to identify the factors that determine different configurations of building resilience. The findings show that responses depended on the nature of incident and the organization's ability to collect, analyze, interpret, and utilize information effectively. Further, an organization's response, which the authors argued reflects their resilience depends on how prepared they are (monitoring internal and external environments to quickly respond to threats) and their capabilities to adapt.
[54]	Conceptual	Focuses on detecting and activating relevant responses within an organization against adversities. This study proposes a resilient response framework, which entails detecting possible threats and taping into relational and cognitive resources to mitigate any consequences on business operations.
[45]	Empirical case study based on publicly available data	Based on an investigation of how some airlines succeeded after the 9/11 attacks, the findings of this study reveal that availability of financial reserves and an available business model are key to resilience and survival after a crisis. Organizations lacking these two often respond to crises with layoffs. While temporarily efficient, layoffs inhibit recovery in the years after a crisis, and perhaps in the long term, because it undermines social relationships needed for long term resilience.
[43]	Conceptual	The authors argue that organizations should be willing to reinvent business models and strategies while anticipating and adjusting to changes in order to build capabilities in strategic resilience. To do this, organizations should address four challenges; conquering denial (avoid illusions of safety and embrace realities of a changing world), valuing variety (e.g., experiment to increase opportunities for stable revenues by expanding sources of revenues), liberating resources (invest in promising ideas), and embracing paradoxes (encourage both exploitation and exploratory strategies and practices).

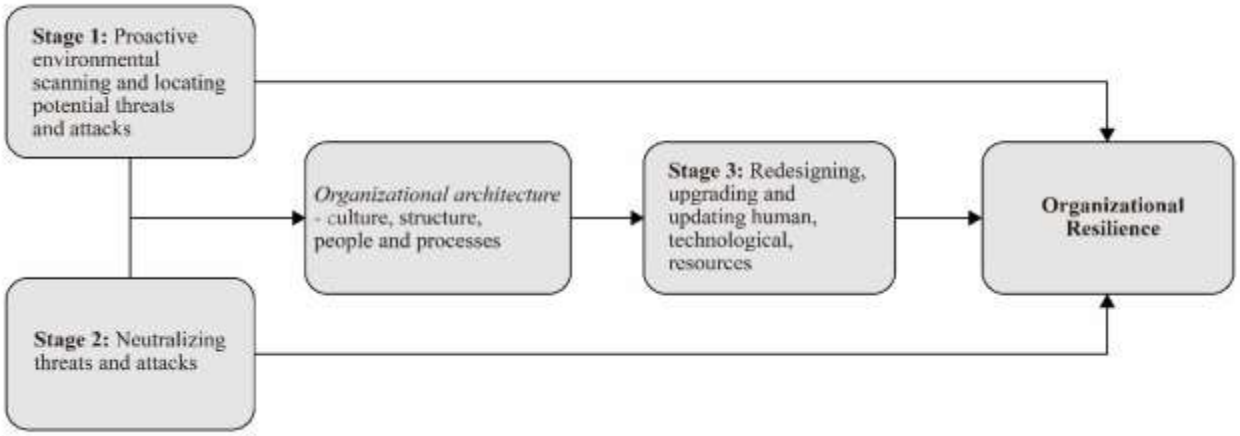

Fig. 1. Organizational resilience model for responding to cyber-attacks

III. DESIGN AND DATA

Following [23], we sourced cases from a wide range of sectors (e.g., telecommunication, travel and transport, governments and local councils, entertainment, health and freight) and countries (e.g., United Kingdom, United Arab Emirates, United States, Singapore, etc.) to collate lessons for resilience. All the cases chosen had recovered after having their operations tremendously affected by a cyber-attack between 2010-2018. To various extents, they had all also demonstrated resilience by ensuring business continuity during the attack. We elucidated common patterns in the responses in line with our model with the aim of equipping organizational leaders with up-to-date expertise to inform decisions that enrich their organizations' approaches and responses to cyber-attacks. The cross-sector and cross-national nature of the cases means that the findings underlying our model are enlightening to many organizations regardless of their culture or location [23]. This approach of highlighting lessons from a wide range of cases has also been found to be particularly effective in bringing new light to existing phenomena [49], [55]. The specific responses presented were sourced from press commentaries and corporate statements made on company websites and blogs (Appendix 1). In all, we identified twenty-one illustrative examples/cases and synthesized the insights in what follows.

A. Stages in Responding to Cyber-attacks: Applications and Examples

In the following section, we employ twenty-one cases of cyber-attacks to buttress the three stages of developing resilience reflected in the dimensions of our model. The cases and relevant background stories are summarized in Appendix 1.

1) Stage 1: Proactive environmental scanning and locating threats and attacks

This stage focuses on scanning and spotting threats and attacks. To exemplify the actions that organizations exhibit in operationalizing this stage, we turn to steps victim-organizations, including the National Health Service (NHS) England, TalkTalk and Carphone Warehouse have undertaken to scan and spot threats.

a) NHS England

In 2017, NHS England was one of the victims of the most widespread cyber-attacks that affected corporations worldwide. WannaCry, as cyber-security experts named this attack, encrypted data on infected computers and made it impossible for users to access their files. In all, 34% of NHS Trusts faced severe disruptions to services. 6, 912 appointments were cancelled, although there were suspicions that a higher number of about 19,000 unrecorded appointments may have been cancelled altogether. A key action that the NHS took in response to this attack was to put in place measures that could help spot future threats. Specifically, the NHS signed a security contract with Microsoft to provide them with a new Microsoft package. This special package was to 'enhance security intelligence' by helping to identify new sources of threats early and making it possible to contain malicious attacks so that they do not spread to other systems [56]. The Health Secretary at the time, Jeremy Hunt endorsed this response, explaining that:

'This new technology will ensure the NHS can use the latest and most resilient software available – something the public rightly expects'.

b) TalkTalk

Two years earlier, customers of TalkTalk, a UK internet service provider, had their personal data compromised following 'a significant and sustained' cyber-attack which was carried out on the company's website. Investigations revealed that TalkTalk had not encrypted the stolen data, making it an easy target for cyber attackers. The information retrieved from customers included credit card and bank account details. As explained by Elizabeth Denham, the Information Commissioner who posed a hefty fine of £400, 000 on TalkTalk,

'*Yes, hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information. It did not and we have taken action'.*

In response and in what seems to be a demonstration of learning its lessons, TalkTalk hired an external, independent party to assess all its processes and security systems to identify areas of vulnerabilities and possible sources of future threats. This was to ensure that the organization was not leaving any crevices for attackers to poach on their cyber-systems.

c) Carphone warehouse

Carphone warehouse, a company that had previously been part of the TalkTalk group, also faced a cyber-attack in 2015 where about three million customer and 1000 employee data were stolen. According to the Financial Times, the attackers capitalized on an outdated WordPress interface, which was still being used by Carphone Warehouse. The UK's Information Commissioner, Elizabeth Denham rebuked this vulnerability the company had opened its customers to, noting that:

'A company as large, well-resourced and established as Carphone Warehouse, should have been actively assessing its data security systems and ensuring systems were robust and not vulnerable to such attacks'.

In response, the company sought external cyber expertise to enhance its cyber security and help make their systems ready to identify in good time, future attempts of cyber-attacks.

d) SingHealth

Elsewhere in Singapore, the country's largest healthcare provider, SingHealth, was the victim of a cyber-attack in 2018. Personal non-medical data, including patient's names, addresses, birthdates and information on identity cards from patients who had visited various health care centers from May 2015 to July 2016 of 1.5 million, were compromised. A worrying finding that emerged from the investigations on this attack related to how staff of the organization had failed to follow up suspicious activities observed in the systems. Thus, while SingHealth put in place measures to enhance the monitoring capabilities of its IT systems to spot possible threats, there was also an emphasis on the need to couple such scanning and monitoring measures with immediate actions to forestall the potential threat.

e) DarkSeoul

In March 2013, cyber-attackers used a malware, called DarkSeoul to carry out an attack on the South Korean government. Various institutions, including the three largest television stations, a bank, ATM machines and mobile payments were affected. Based on previous evidence of cyber-attacks, South Korea censured North Korea for this particular attack. Since the attack, cyber-security has become one of the core policy areas of the South Korean Government. Media reports suggest that the Government has particularly invested in sophisticated monitoring systems to spot future attempts of cyber-crimes.

These cases exemplify various organizational attempts to scan and spot cyber threats and attacks. Together, they point to some of the early practices which we consider important in building a resilient model against cyber-attacks. It is worth noting that all the specific practices outlined here, encrypting data, assessing vulnerabilities of cyber systems and putting in place software that helps to detect threats, may not be able to avoid attacks. The CEO of the Copeland Council, Ms. Graham, after it had been hit by cyber attackers underscored this point, noting that '*There is no way we could have kept this attack out, but had we had great IT investment we probably would have recovered quicker*.' Thus, the examples mentioned above should be aimed at identifying threats and possible attacks and containing them, in a way that ensures business continuity. To ensure business continuity when a threat or attack is discovered, organizations need to neutralizing effects.

2) Stage 2: Neutralizing threats and attacks

The second stage focuses on tactical responses adopted by firms when an attack happens, i.e., responses at the trans-attack phase, or when a threat is spotted. Organizational scholars have increasingly been concerned about cyber-attacks in the wake of increasing technological advancements in data collection, data access and technology for illegal access to others' data. From our findings, it appeared that organizational responses to cyber-attacks aimed at recovery was the most crucial to prevent cyber-attacks from crumbling an organization's operations. To illustrate the actions entailed in neutralizing current and threats, we turn to the following cases: Maersk, Atlanta City Council, Instagram, Uber, Sony Pictures, Cathay Pacific, and Careem.

a) Maersk

In June 2017, Maersk was one of the victims of a cyber-attack, called Notpetya. This attack was carried out by Russia against Ukrainian organizations and organizations with offices in Ukraine. The attack, which prevented employees of affected organizations from accessing their data, affected Maersk

Line, APM Terminals and all business units of Maersk. The attackers requested a ransom payment of $300 in Bitcoin, which Maersk refused to pay. Management of Maersk, explaining their plans for the future, noted that given the sophisticated nature of cyber-attacks, it may not always be possible to completely prevent a future attack. They considered that preparing an effective recovery strategy would be the most relevant option. One of the most important steps it took when the attack happened was, thus, to ensure that it mitigated the consequences of the attack on its operations. To achieve this, information on which of its activities were running or closed and at what times (such as loading times in ports and booking systems), were shared to all relevant parties. The organization also developed a new makeshift booking system to ensure continuous running of essential operations. Finally, according to Sonen Skou, Maersk's CEO, all frontline employees were quickly empowered to respond to customer needs in what they considered to be the best possible way, 'do what you think is right to serve the customer — don't wait for the headquarters, we'll accept the cost' [57]. On a more general scope, Maersk reviewed their systems to become more resilient by introducing new measures to enhance cyber-security so that in the event of a reoccurrence, it would be able to 'isolate an attack quicker and restore systems quicker' [57].

b) Atlanta City Council

A year after the Maersk attack, the Atlanta City Council, US, was also affected by a cyber-attack that infiltrated the bulk of the municipal's systems. The attackers demanded a ransom payment of approximately $50,000 in bitcoin, which the City Council refused to pay in line with the FBI directives. As a result of the attack, about 424 of the City's software could not operate online. Residents could not undertake basic public tasks that relied on the City's systems, such as paying for parking tickets and utility bills. The Council's first response was to direct all employees to turn off their computers. This simple directive was to prevent further spread of the ransomware through its networks. An additional emergency measure the Council took to neutralize the attack was to deploy a number of external contracts

to offer some of its services that had been affected. Specifically, the Council entered into about ten contracts with external agencies and institutions to be able to provide the affected services.

c) Instagram

Instagram's response to a cyber-attack on its systems also offers a demonstration of how organizations may neutralize the effects of a cyber-attack. In August 2018, cyber attackers replaced Instagram users' account details, including profile images, handles, contact details and bios, with still photos from Disney movies. They also replaced email addresses with ones ending with .ru, a Russian domain. While the organization's investigations found that most of the hacked accounts were not two-factor secured, it was also found that some users' who had done two-factor authentication were still affected. When Instagram had received information about the attack, they quickly sent out instructions to Instagram users and guided them on securing their data. Users were informed to '*report any unusual activity through our reporting tools. You can access those tools by tapping the '…' menu from your profile, selecting 'Report a Problem' and then 'Spam or Abuse'*. The social media company also explained that they had fixed the bug immediately they found out about it and cooperated with law enforcement agencies for further investigations.

d) Uber

A fourth example of how organizations neutralize such attacks can be seen in the response of Uber, a ride-hailing service after it became victim for the second time to cyber-attacks. Hackers broke into Uber's GitHub account and stole information, including names, email addresses, phone numbers and drivers' license numbers, from about 57 million customers and drivers in 2016. According to the CEO, the hackers used a third-party cloud-based service to carry out the attack. While legal regulations ban cyber victims from paying ransoms to attackers, Uber paid an initial $100,000 to the attackers to destroy the data they had stolen. In addition, the CEO claimed that Uber:

'*Took immediate steps to secure the data and shut down further unauthorized access by the individuals. We also implemented security measures to restrict access to and strengthen controls on our cloud-based storage accounts*' (CEO, cited in Newcomer 2017).

e) Cathay Pacific

In October 2018, Cathay Pacific was the victim of a cyber-attack that leaked personal information, such as names, identity card numbers, passport details, email addresses and credit card details of about 9.4 million passengers. Even though the attack was spotted during a routine IT operation the organization was carrying out, investigations revealed that the data breach had been going on for much longer. Cathay Pacific's focus for the first three months of the attack was directed towards containing it. All affected customers were informed of the attack and offered guidance on how to protect themselves, including an option for complementary monitoring. A dedicated website was also set up for customers to communicate with the organization on their concerns. In a video placed on their website, CEO, Rupert Hogg confirmed these strategic activities:

'*Upon discovery, we acted immediately to contain the event and to thoroughly investigate…We engaged one of the world's leading cybersecurity firms to assist us and we further strengthened our IT security systems too*' (Rupert Hogg, CEO, 2018).

f) Sony pictures

Sony pictures faced a massive cyber-attack, Wannacry, in October 2014. The attackers accessed and shared yet-to-be released movies on illegal sites and stole confidential information belonging to Sony Pictures and individual employees, which they then circulated online. Employees could not use their computers for more than six weeks after the attack for fear of remnants affecting their online activities. One of Sony's first responses was to provide security and protection to top producers and actors linked

to the movie titled, The Interview. This was in response to threats of physical abuse from the attackers. It also offered a year of credit monitoring to current employees. Sony's legal partners asked all media houses to stop further downloading information that had been compromised and also to destroy any data they already had in their possession. Using the services of third-party companies, like Entura International Limited, Sony Pictures tried to block distribution of the stolen data and to delete all links that lead to the hacked information.

g) Careem

In 2018, information from about 14 million customers and drivers of Careem, a ride-hailing app, operating in countries in the Middle East, were stolen. The affected information included ride histories, names, phone numbers, credit card details and email addresses. Careem got to know about the attack based on a note the attacker left on their system. According to Forbes Middle East [58], the main impact of this attack is the erosion of trust by customers that Careem and all other online based transactions are likely to confront. This is especially so because the Middle East is still emerging in the use of online transactions and customers may be discouraged on the security of their systems. Careem took immediate measures to neutralize the effects of the attack as explained below;

> '*As soon as we detected the breach, we launched a thorough investigation and engaged leading cybersecurity experts to assist us in strengthening our security systems. We are also working with law enforcement agencies. Throughout the incident, our priority has been to protect the data and privacy of our customers and captains. Since discovering the issue, we have worked to understand what happened, who was affected and what we needed to do to strengthen our network defenses.*' (Careem Official Blog Post, 2018)

While the first stage of scanning and identifying sources of threats are important, the sentiments shared by individuals who have led their organizations through cyber-attacks, demonstrate that such steps

are not always sufficient in forestalling attacks. Instead, we observe that it is the second stage, characterized by recovery efforts or tactical responses to the attacks that often fortify the victim-organizations and make them resilient under the pressure of the effects of the attack.

3) Stage 3: re-designing, upgrading and updating human, technological and financial resources

In line with the third stage of our model, organizations usually undertake a more long-term approach towards building resilience. This section shares some lessons from organizations that have taken a long-term approach in avoiding such attacks.

a) TalkTalk

After the 2015 cyber-attack on TalkTalk, the internet provider announced that it had invested more in security of its cyber systems for future resilience. In addition, the organization reported that cyber security had been integrated into the whole organization, rather than as a separate business function:

> '*Security is discussed at every meeting and is embedded in everything we do with the products and the services that we launch and has become part of the day to day discussion…we currently have an online training system with all our staff going through training programs making sure employees are aware of all the types of security and risk and what we would expect in terms of a secure approach*…' (Duncan Gooding, COO, TalkTalk, 2017).

b) Google China

Similarly, in 2010, cyber-attackers hacked into Google China's Office Systems and retrieved system codes. According to McAfee, the highly sophisticated attack, 'Operation Aurora', used about 12 different malwares and several levels of encryption to ransack the company's networks. Further investigations by Google revealed that some Gmail accounts had also been compromised, although the

attackers seemed to have only gained access to account details, such as email addresses and subject titles, rather than content of emails. In response to the attack, the multinational built more efficient infrastructure and architecture to enhance security of its systems. Google also initiated a worldwide educational campaign for its users, informing them on ways to protect themselves from attacks, through for instance, using proper antivirus programs. Most significantly, Google China moved its servers to Hong Kong, where there were no internet filtering policies.

c) SingHealth

In a recent case, cyber-attackers stole non-medical records of about 1.5 million people from SingHealth, the largest health group institution in Singapore. The stolen data included medical details of the Prime Minister and some other ministers. In response, the IHiS drew on external expertise to evaluate cybersecurity policies, threat management processes, IT system controls and organizational and staff capabilities of systems within public health care institutions. Another measure taken was to educate both public and private healthcare institutions on ways of protecting themselves against cyber-attacks. Regardless of these efforts, the Minister of Health noted that it will be impossible to completely eliminate the risk of another cybersecurity attack. As already noted, this is a sentiment that is shared by most organizations that have been victims of cyber-attacks. The consensus appears to be that it may be difficult to put in place long-term mechanisms to avoid such problems.

d) Uber

Uber (described in Stage 2) had planned to massively invest into improving security and specifically protecting their systems against further hack attempts. It was expected that about 75 more employees would be recruited to support the work of the security team. In addition, the organization made significant progress by recruiting a new Chief Security Officer, Joe Sullivan, who was previously a federal prosecutor of cyber-crime. Joe Sullivan promised to leverage on technology to improve cyber

security as well as security against physical threats, trust and safety of customers. The new CSO, Joe Sullivan, also noted plans to monitor the use of data even by employees of Uber across the world in order to prevent abuse of customers' data. As he noted,

> '*Every company is a data company now, no one can be unsophisticated. The challenge is half the company needs access to customer data some of the time — it is not just customer support, it is marketing, engineers as they iterate, communications when they need to figure out what happened in an incident.*' (Joe Sullivan, CSO, Uber, 2015).

In response to the problem this poses, the organization now runs random data auditing to ensure that employees are only accessing data when necessary and for its intended purposes.

The cases in this stage suggest that as part of building their resilience, organizations often put in place long term measures to guide themselves against possible future attacks. The activities at this stage are often extremely comprehensive and may require wholly reconfiguring certain organizational processes and systems.

IV. GENERAL DISCUSSION, IMPLICATIONS AND SUGGESTIONS

We proposed a model of organizational resilience, identifying how organizations can analyze, mobilize and revise their processes to become more resilient. We then drew on examples of cases to shed light on the specific actions that can be taken in each stage of the model. Although the cases vary in internal characteristics, such as in organizational culture, structure and business processes, and external characteristics, such as motive behind attacks, there are still significant and clear commonalities in terms of responses and resulting lessons for organizations seeking to be resilient in an era of cyber adversities. In what follows, and supported by relevant literature, we reiterate the lessons and recommendations from

each of the stages, as shown in Table 2. Next, we highlight the contributions of our study to existing literature, identify limitations and corresponding directions for future research.

TABLE II
RESILIENCE ARCHITECTURE MODEL: FINDINGS AND LESSONS

Focus of resilience model	**Resilient practices and suggested responses**	**Relevant studies**
Proactive environmental scanning and locating potential threats – *Focus on period before an attack or threat is discovered*	- Anticipate possibilities for attacks - Regularly scan and monitor systems for threats and attacks - Utilize internal expertise of hire external expertise to assess vulnerabilities	[11], [23], [50]
Neutralizing threats and attacks – *Focus on period an attack or threat is discovered. Aimed at stopping a threat, containing an attack, and reducing the effect of an attack on the organization's activities*	- Empower frontline employees to respond to customer needs - Regularly provide information to relevant and key stakeholders on measures that need taking (e.g., available and unavailable services) - Deploy external agencies and partners to offer core services - Communicate with affected customers on how to secure their data and offer incentives to discourage switching to unaffected competitors - Utilize available expertise to help contain attack and curtail distribution of the stolen data - Purchase new cyber systems to ensure normal business functioning - Make insurance claims to cover costs or tap into other financial reserves	[13], [20], [21], [26], [31], [45], [50], [59]
Re-designing, upgrading and updating human, technological and financial resources – *Focus on putting in place ongoing and long-term strategies to manage cyber-attacks.*	- Make cyber security efforts integral to all parts of the organization - Invest in more efficient cyber infrastructure - Conduct regular auditing of cyber systems and where needed, hire external to help regularly evaluate cyber systems - Train all employees to be clear on roles and responsibilities in managing cyber security - Have favorable insurance policies in place - Ensure regular upgrading of financial reserves - Encourage flexible and viable business models	[21], [26], [31], [36], [41], [42], [45], [46]

A) Key lessons and recommendations for organizations

1) Stage 1

In an environment rife with uncertainty, organizations need to proactively scan their environment for threats and where possible, translate them into strategic flexibilities. At the scanning and spotting stage of the resilient model, organizations undertake deliberate actions to detect threats [60]. This is important to reduce blind spots and ensure relevant latent resources are activated to respond effectively to attacks [11], [20]. As the illustrations from our cases suggest, attacks sometimes festered and caused damage in organizations' systems for as long as two years, without victims' awareness. Thus, a common concern that organizations have is how to assess cyber systems to spot looming threats or attacks quickly. An important practice is for managers to ensure that regular and routine checks are conducted to identify any discrepancies in systems' operations. As the examples from NHS and SingHealth show, organizations may benefit from updated cyber interfaces and personalized software that automatically scans threats in cyber systems. However, as demonstrated in the case of the apathetic employees in SingHealth, it is not enough to scan and spot suspicious activities. Employees also need to be sensitized to respond or report such activities immediately upon discovery. Scanning could also be aimed at evaluating cyber systems for vulnerabilities [26]. Where such vulnerabilities or weaknesses, rather than threats or attacks are spotted, organizations need relevant expertise to advice on ways of securing systems and avoiding an attack. As Crichton et al. [23] advice, however, organizations should be aware of such 'preparedness' giving a false sense of security, which often leads to disregarding other relevant actions. The resulting complacency often leads to devastating outcomes when an adversity happens.

2) Stage 2

When an attack or threat has been spotted, relevant responses should immediately be activated to contain complications and neutralize effects on business operations [60]. These responses are tactical in

nature and are the most important for surviving through attacks. The aim here, in line with expectations of resilient organizations is to persevere through the attack and ensure business continuity [16], [20]. At this stage, a number of practices and responses suggested in the resilient literature and demonstrated by our case examples are essential. (1) There is an indisputable need to work closely with security agencies and where available, government offices in charge of cybersecurity, such as the UK's National Cyber Security Centre. (2) Organizations will need to tap into resources of external networks and alliances [44], [59]. This is especially vital when they need to hire temporary workers or expertise to help in recovery processes or to maintain delivery of essential services, in times when cyber-attacks leave their systems inoperable. The responses from Copeland Council and the City of Atlanta illustrate how external agencies and expertise could be useful for ensuring business continuity at this stage. (3) A third important response at this stage is dissuading customers, especially where they have been directly affected by an attack, from switching to competitors. In the first attack against TalkTalk, thousands of customers immediately switched to other internet service providers. To reduce similar incidents, the neutralizing stage requires resilient organizations to aggressively seek to maintain their customer base. As demonstrated in our cases, Anthem Insurers offered two years of credit monitoring, while BA offered financial compensation for customers whose accounts had been affected. (4) A fourth crucial practice that can make organizations resilient during attacks is to constantly communicate updates to affected parties in a professional manner, as demonstrated by most of the twenty-one cases. The communication needs to be clear, accessible, relevant and reasonably regular. In relation to this, frontline employees should be empowered to offer relevant solutions and responses to customers. (5) Furthermore, organizations also need to create robust back-up systems that enable them to recover loss data and switch to different systems that enable them to continue to maintain momentum or function to successfully neutralize the effects of an attack. (6) Finally, organizations should be ready to invest in new systems to ensure ongoing delivery of services, such as in the case of Maersk for example, where the organization urgently installed 4,000 new servers,

45,000 new PCs and 2,500 applications. To defray these costs, organizations may benefit from tapping into favorable insurance packages [35], [53] as demonstrated in how Equifax planned to handle its costs.

3) Stage 3

At the third stage of the resilient model, organizational responses are more strategic in nature and aimed at making resilience to cyber-attacks an integral part of the day to day activities of the organization for long term benefits [31]. As the CEO of TalkTalk explained, one of the responses the organization has taken to become more resilient against cyber-attacks is by regularly discussing cyber security issues at meetings and embedding security practices in all processes relating to products and services. A barrier to reducing the impact of attacks is the lack of dedicated resources to identify and respond to weakness in organizations' systems. This also affects the post-attack phase and ability of firms to benefit from the recovery strategies outlined in Stage 2. To address this, investment in human resources and empowering them to mobilize and implement relevant expertise is again, crucial [36], [46]. (1) There is a need to expand employees' consideration of threats to include cyber threats as an evolving and re-occurring danger to businesses. In this regard, many of our case organizations had indicated skills upgrading as an essential means of developing strategic flexibility. Financial and non-financial reward systems may be instituted for tech-savvy individuals to report new threats and weaknesses in systems. (2) In addition, organizations need to be deliberate at investing financial resources and updating technological resources specifically for the purposes of managing cyber threats. According to [45], having financial reserves prevents layoffs, and in turn helps sustain strong social bonds within the organization which is crucial for persevering through crises. Cyber insurance policies can also be an important strategic response to fund responses. (3) Finally, flexibility in business models is crucial to enable organizations adapt routines and processes in response to vulnerabilities and attacks [41], while viable business models (e.g. ensuring low cost of operations), can help save towards adversities [45].

It is worth noting that the three stages of resilience are neither mutually exclusive nor strictly linearly progressive. For instance, organizations need not have been attacked to start updating or re-designing their human, financial and technological resources. In fact, attention paid to effective strategic measures, outlined at the third stage, will ensure quick recovery when responses relevant for neutralizing the effects of an attack are activated during an attack. In addition, certain actions and responses are important across all stages of the model, even though we found that they were commonly present in specific stages of the organizations' studied responses. For instance, scanning cyber systems for threats and attacks could still be important even when an attack has happened. This is because cyber systems become particularly vulnerable in the midst of ongoing attacks and an easy target for cyber criminals to infiltrate other parts of an organizations systems.

How do organizations incorporate these lessons into achieving an effective architecture for resilience against cyber-attacks? On a broader level, organizations must ensure that their processes, people, culture and strategies are creatively aligned to support relevant responses and actions highlighted in the three stages. Importantly, and based on existing studies and our findings, we suggest that the architecture is 1) flexible and innovative to accommodate changes, 2) regularly evaluated to update processes and practices in response to feedback from various stages of the model, and 3) integral across all facets of the organization. These, while uncomfortable and costly for some organizations, are essential to reduce the extent to which threats or attacks from cyber criminals that impact on business goals. Fortunately, when well-integrated to all functions of the organization, the benefits of resilience go beyond making organizations robust against cyber-attacks. Such an architecture could also be an effective source of competitive advantage. In addition, organizations differ in organizational structure and business processes. Thus, although, it was not the focus of this study to offer micro perspectives regarding the moderation effects of organization characteristics on the strategic implementations of the three stages,

managers are encouraged to carefully evaluate and take these differences into account in strategic planning.

B) Contributions, limitations, and suggestions for future studies

In addition to the practical relevance of our paper for practicing managers, our research also contributes to the literature on cyber-attacks and resilience. First, in direct response to contextual gaps spotted in a recent review of influential studies on resilience management [20], our paper integrates insights on resilience from different domains and apply them to the unique context of adversities linked to cyber systems. In particular, our cross-sector cases have provided new insights into the previous unseen 'methods' [21] of how resilience against cyber-attacks happens in organizations. Second and relatedly, by situating our study in the complex and unpredictable context of cyber-attacks where complete avoidance of an attack through traditional risk assessments is near impossible [21], this study confirms the need for definitions that recognize context specific strengths and emergent meanings of resilience [20]. Specifically, the ways in which our case organizations demonstrated resilience through ensuring business continuity through attacks offers support to definitions of resilience as robustness and perseverance through adversities [22], rather than complete avoidance.

Given the dearth of knowledge on practical responses resilient organizations undertake in responding to cyber-attacks, we have focused here on cyber-attacks. However, our model also seems to be of broad relevance to organizations seeking to develop resilience against other forms of environmental upheavals. This is because in articulating practices relevant for our model through the cases, we emphasized soft managerial skills, such as dissuading customers from switching during a crisis, and other considerations that resonate with the day-to-day running of organizations peculiar to contemporary business environments. All of these are accessible and practically relevant to managers whose organizations are faced with various adverse situations. Our study has, thus, progressed some way

towards responding to a key research question in a review by Linnenluecke [20, p23] on 'how findings from discrete case examples could be integrated to develop insights that are more generalizable to different settings and contexts'.

Despite the insights from our study, it is not without limitations. First, as a result of relying on commentaries on how organizations have responded to cyber-attacks from affected organizations' own websites, PR outlets as well as press information, there are possibilities for bias in some of the information available. It is, for instance, possible for some of these responses to have been framed by organizations to appease affected audience and protect organizational reputation, while withholding actual ways in which they responded [61]. We have, where possible, relied on more than one source of information for the cases as an attempt to reduce such incidents of strategic framing. For future research, data collected through direct interviews and surveys with multiple parties involved or affected could be useful. Second, while our lessons may be useful for organizations of different sizes, we believe that further studies focusing on smaller businesses can add new insights to some of the lessons enumerated here. This is because, the unique behavioral tendencies and resource constraints of small businesses may necessitate different responses to the ones the mainly large organizations illustrated in our study adopted. An insightful finding relates to how relationships with external parties can be an important avenue to persevere through cyber adversities. Going forward with research in the area, it will be interesting to examine the value of political ties and pressure groups in combatting these attacks. This is particularly important as cyber-attackers seem to, themselves, be often motivated by political ambitions, such as in the suspected cases of 'Lazarus', a North Korean Government group's attack against Sony Pictures, the Chinese Government against Google's China platform to stall human right actions, and Russian agents attack against Maersk (and other Organizations operating in Ukraine).

REFERENCES

[1] J. Czinkota, M. R., Knight, G., Liesch, P. W., Steen, 'Terrorism and international business: A research agenda,' *J. Int. Bus. Stud.*, vol. 41, no. 5, pp. 826–843, 2010.

[2] A. Bendovschi, 'Cyber-attacks–trends, patterns and security countermeasures,' *Procedia Econ. Financ.*, vol. 28, pp. 24–31, 2015.

[3] K. A. Whitler and P. W. Farris, 'The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches,' *J. Advert. Res.*, vol. 57, no. 1, pp. 3–9, 2017.

[4] E. Al Mazari, A., Anjariny, A. H., Habib, S. A., Nyakwende, *Cyber terrorism taxonomies: Definition, targets, patterns, risk factors and mitigation strategies*, 1st ed. Pennsylvania: IGI Global, 2018.

[5] P. Ceric, A., Holland, 'The role of cognitive biases in anticipating and responding to cyber-attacks,' *Inf. Technol. People*, vol. 32, no. 1, pp. 171–188, 2019.

[6] J. A. Lewis, *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic and International Studies, 2002.

[7] B. Rid, T., Buchanan, 'Attributing cyber attacks,' *J. Strateg. Stud.*, vol. 38, no. 1–2, pp. 4–37, 2015.

[8] S. K. G. D'Aveni, R. A., Dagnino, G. B., 'The age of temporary advantage,' *Strateg. Manag. J.*, vol. 31, no. 13, pp. 1371–1385, 2010.

[9] V. Sambamurthy, V., Bharadwaj, A., Grover, 'Shaping agility through digital options: Reconceptualizing the role of IT in contemporary firms,' *MIS Q.*, vol. 27, no. 2, pp. 237–263, 2003.

[10] X. Sheng, J., Amankwah-Amoah, J., Wang, 'A multidisciplinary perspective of big data in management research,' *Int. J. Prod. Econ.*, vol. 191, pp. 97–112, 2017.

[11] D. Gligor, N. Gligor, M. Holcomb, and S. Bozkurt, 'Distinguishing between the concepts of supply chain agility and resilience: A multidisciplinary literature review,' *Int. J. Logist. Manag.*, vol. 30, no. 2, pp. 467–487, 2019.

[12] R. Kupers, 'Resilience in complex organizations,' *The Global Risks Report 2018 13th Edition, Work Economic Forum*, 2020. [Online]. Available: https://reports.weforum.org/global-risks-2018/resilience-in-complex-organizations/.

[13] S. McManus, E. Seville, D. Brunsdon, and J. Vargo, 'Resilience management: A framework for assessing and improving the resilience of organisations,' 2007.

[14] Liu, Y., J. Wei, D. Zhou, Y. Ying, and B. Huo, 'The alignment of service architecture and organizational structure,' *Serv. Ind. J.*, vol. 36, no. 9–10, pp. 396–451, 2016.

[15] M. T. Britto *et al.*, 'Using a network organisational architecture to support the development of Learning Healthcare Systems,' *BMJ Qual. Saf.*, vol. 27, no. 11, pp. 937–946, 2018.

[16] F. Björck, M. Henkel, J. Stirna, and J. Zdravkovic, *Cyber resilience–fundamentals for a definition*. Cham: Springer, 2015.

[17] H. Goldman, R. McQuaid, and J. Picciotto, 'Cyber resilience for mission assurance,' in *IEEE International Conference on Technologies for Homeland Security (HST)*, 2011, pp. 236–241.

[18] C. A. Beck, T. E., Lengnick-Hall, 'Resilience capacity and strategic agility: Prerequisites for

thriving in a dynamic environment,' 2016.

[19] V. G. Dubey, R., Ali, S. S., Aital, P., Venkatesh, 'Mechanics of humanitarian supply chain agility and resilience and its empirical validation,' *Int. J. Serv. Oper. Manag.*, vol. 17, no. 4, pp. 367–384, 2014.

[20] M. K. Linnenluecke, 'Resilience in business and management research: A review of influential publications and a research agenda,' *Int. J. Manag. Rev.*, vol. 19, no. 1, pp. 4–30, 2017.

[21] L. I. and K. A, 'Fundamental concepts of cyber resilience: Introduction and overview,' in *Kott A., Linkov I. (eds) Cyber Resilience of Systems and Networks. Risk, Systems and Decisions*, Springer, Ed. Cham, 2019, pp. 1–25.

[22] A. Annarelli and F. Nonino, 'Strategic and operational management of organizational resilience: Current state of research and future directions,' *Omega*, vol. 62, pp. 1–18, 2016.

[23] M. T. Crichton, C. G. Ramsay, and T. Kelly, 'Enhancing organizational resilience through emergency planning: learnings from cross-sectoral lessons,' *J. Contingencies Cris. Manag.*, vol. 17, no. 1, pp. 24–37, 2009.

[24] G. M. Caporale, W. Y. Kang, F. Spagnolo, and N. Spagnolo, 'Cyber-attacks and cryptocurrencies,' Munich, 2020.

[25] M. Uma and G. Padmavathi, 'A Survey on Various Cyber Attacks and their Classification,' *Int. J. Netw. Secur.*, vol. 15, no. 5, pp. 390–396, 2013.

[26] A. Ghadge, M. Weib, N. Caldwell, and R. L. Wilding, 'Managing cyber risk in supply chains: A review and research agenda,' *Supply Chain Manag.*, vol. 25, no. 2, pp. 223–240, 2019.

[27] I. N. Fovino, M. Masera, and A. De Cian, 'Integrating cyber attacks within fault trees,' *Reliab. Eng. Syst. Saf.*, vol. 94, no. 9, pp. 1394–1402, 2009.

[28] Koike, H., K. Ohno, and K. Koizumi, 'Visualizing cyber attacks using IP matrix,' in *IEEE Workshop on Visualization for Computer Security*, 2005, pp. 91–98.

[29] G. Hug and J. A. Giampapa, 'Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks,' *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, 2012.

[30] H. Li, X., Liang, X., Lu, R., Shen, X., Lin, X., Zhu, 'Securing smart grid: cyber attacks, countermeasures and challenges,' *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 38–45, 2012.

[31] B. Sheppard, M. Crannell, and J. Moulton, 'Cyber first aid: proactive risk management and decision-making,' *Environ. Syst. Decis.*, vol. 33, no. 4, pp. 530–535, 2013.

[32] C. van Hardeveld, G. J. Webber and K. O'Hara, 'Deviating from the cybercriminal script: exploring tools of anonymity (mis) used by carders on cryptomarkets,' *Am. Behav. Sci.*, vol. 61, no. 11, pp. 1244–1266, 2017.

[33] S. McCombie, 'Threat actor oriented strategy: Knowing your enemy to better defend, detect and respond to cyber-attacks,' *J. Aust. Inst. Prof. Intell. Off.*, vol. 26, no. 1, pp. 24–41, 2018.

[34] A. Davis, 'Building cyber-resilience into supply chains,' *Technol. Innov. Manag. Rev.*, vol. 5, no. 4, pp. 19–27, 2015.

[35] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, 'ontent analysis of cyber insurance policies: how do carriers price cyber risk?,' *J. Cybersecurity*, vol. 5, no. 1, p. tyz002, 2019.

[36] M. L. Lengnick-Hall, C. A., Beck, T. E., Lengnick-Hall, 'Developing a capacity for organizational resilience through strategic human resource management,' *Hum. Resour. Manag. Rev.*, vol. 21, no. 3, pp. 243–255, 2011.

[37] G. Bustinza, O. F., Vendrell-Herrero, F., Perez-Arostegui, M., Parry, 'Technological capabilities, resilience capabilities and organizational effectiveness,' *Int. J. Hum. Resour. Manag.*, pp. 1–23, 2016.

[38] K. Burnard, R. Bhamra, and C. Tsinopoulos, 'Building organizational resilience: Four configurations,' *IEEE Trans. Eng. Manag.*, vol. 65, no. 3, pp. 351–362, 2018.

[39] L. K. Comfort, *Shared Risk: Complex Systems in Seismic Response*. New York: Pergamon, 1999.

[40] T. A. Williams, D. A. Gruber, K. M. Sutcliffe, D. A. Shepherd, and E. Y. Zhao, 'Organizational response to adversity: Fusing crisis management and resilience research streams,' *Acad. Manag. Ann.*, vol. 11, no. 2, 2017.

[41] C. Carayannis, E. G., Grigoroudis, E., Sindakis, S., Walter, 'Business model innovation as antecedent of sustainable enterprise excellence and resilience,' *J. Knowl. Econ.*, vol. 5, no. 3, pp. 440–463, 2014.

[42] L. H. Birchall, J., Ketilson, *Resilience of the cooperative business model in times of crisis*. Geneva, Switzerland: International Labour Organization, Sustainable Enterprise Programme, 2009.

[43] G. Hamel and L. Välikangas, 'The quest for resilience,' *Harv. Bus. Rev.*, vol. 81, no. 9, pp. 52–63, 2003.

[44] W. G. Xavier, R. Bandeira-de-Mello, and R. Marcon, 'Institutional environment and Business Groups' resilience in Brazil,' *J. Bus. Res.*, vol. 67, no. 5, pp. 900–907, 2014.

[45] J. H. Gittell, K. Cameron, S. Lim, and V. Rivas, 'Relationships, layoffs, and organizational resilience: Airline industry responses to September 11,' *J. Appl. Behav. Sci.*, vol. 42, no. 3, pp. 300–329, 2006.

[46] J. G. Levitt, B., March, 'Organizational learning,' *Annu. Rev. Sociol.*, vol. 14, pp. 319–340, 1988.

[47] M. Erol, O., Sauser, B., Mansouri, 'A framework for investigation into extended enterprise resilience,' *Enterp. Inf. Syst.*, vol. 4, no. 2, pp. 111–136, 2010.

[48] R. Rajesh, 'Technological capabilities and supply chain resilience of firms: A relational analysis using Total Interpretive Structural Modeling (TISM),' *Technol. Forecast. Soc. Change*, vol. 118, pp. 161–169, 2017.

[49] M. Groh, 'Strategic Management in Times of Crisis,' *Am. J. Econ. Bus. Adm.*, vol. 6, no. 2, pp. 49–57.

[50] C. L. Bouwens and R. B. Stafford, 'The role of organizational resilience across the cyber attack lifecycle,' in *The International Annual Conference of the American Society for Engineering Management*, 2019.

[51] K. Burnard and R. Bhamra, 'International Journal of Production Research,' *Organ. Resil. Dev. a Concept. Framew. Organ. responses*, vol. 49, no. 18, pp. 5581–5599, 2011.

[52] J. G. Cyert, R. M., March, *A behavioral theory of the firm*. N.J.: Prentice-Hall: Englewood Cliffs, 1963.

[53] M. Camillo, 'Cyber risk and the changing role of insurance,' *J. Cyber Policy*, vol. 2, no. 1, pp. 53–63, 2017.

[54] K. Bhamra, R., Dani, S., Burnard, 'Resilience: the concept, a literature review and future directions,' *Int. J. Prod. Res.*, vol. 49, no. 18, pp. 5375–5393, 2011.

[55] J. Amankwah-Amoah and C. Durugbo, 'The rise and fall of technology companies: The evolutional phase model of ST-Ericsson's dissolution,' *Technol. Forecast. Soc. Change*, vol. 102, pp. 21–33, 2016.

[56] L. Dearden, ‘NHS to spend £150m on cyber security to bolster defences after WannaCry attack,’ 2018. .

[57] R. Milne, ‘Maersk CEO Soren Skou on surviving a cyber-attack,’ 2017. [Online]. Available: https://www.ft.com/content/785711bc-7c1b-11e7-9108-edda0bcbc928. [Accessed: 23-Nov-2018].

[58] Forbes Middle East, ‘Why ride-sharing app Careem’s data hack can be a blow to region’s online payments market,’ 2018. .

[59] L. M. Camarinha-Matos, ‘Collaborative networks: A mechanism for enterprise agility and resilience,’ in *Mertins K., Bénaben F., Poler R., Bourrières JP. (eds) Enterprise Interoperability VI. Proceedings of the I-ESA Conferences*, 2014.

[60] C. L. Bouwens and R. B. Stafford, ‘The role of organizational resilience across the cyber attack lifecycle,’ in *the International Annual Conference of the American Society for Engineering Management*, 2011, pp. 1–8.

[61] S. Shultz, K. C. Opie, and Q. D. Atkinson, ‘Stepwise evolution of stable sociality in primates,’ *Nature*, vol. 479, pp. 219–222, 2011.

[62] M. Field, ‘Six million Instagram accounts hacked: how to protect yourself,’ 2018. [Online]. Available: https://www.telegraph.co.uk/technology/2017/09/04/six-million-instagram-accounts-hacked-protect/. [Accessed: 11-Oct-2018].

[63] G. Wilford, ‘Millions of instagram users may have been affected by latest hack attack, social media giant warns,’ 2017. [Online]. Available: https://www.independent.co.uk/life-style/gadgets-and-tech/instagram-cyber-attack-hack-celebrities-selena-gomez-justine-bieber-millions-ordinary-social-media-a7926211.html. [Accessed: 04-Oct-2018].

[64] J. Davey, ‘Britain’s Dixons Carphone suffers cyber-attack on customer data,’ 2018. [Online]. Available: https://uk.reuters.com/article/us-dixons-carphone-cybercrime/britains-dixons-carphone-suffers-cyber-attack-on-customer-data-idUKKBN1J90OL. [Accessed: 12-Nov-2018].

[65] T. Davies, ‘Marriott hotel chain reveals major cyber attack,’ 2018. [Online]. Available: https://gdpr.report/news/2018/12/03/marriott-hotel-chain-reveals-major-cyber-attack/. [Accessed: 09-Apr-2019].

[66] C. Dobinson, ‘TalkTalk Business COO Duncan Gooding on security strategy since 2015 cyber-attack,’ 2017. .

[67] N. Dludla, ‘South Africa’s Liberty Holdings suffers cyber-attack,’ 2018. [Online]. Available: https://af.reuters.com/article/topNews/idAFKBN1JE0JS-OZATP. [Accessed: 21-Nov-2018].

[68] M. Erman, ‘Merck cyber attack may cost insurers $275 million: Verisk’s PCS,’ 2017. [Online]. Available: https://www.reuters.com/article/us-merck-co-cyber-insurance/merck-cyber-attack-may-cost-insurers-275-million-verisks-pcs-idUSKBN1CO2NP. [Accessed: 24-Nov-2018].

[69] Equifax, ‘Cyber security incident – information for UK customers,’ 2017. .

[70] S. Farall, ‘TalkTalk counts costs of cyber-attacks,’ 2016. [Online]. Available: https://www.theguardian.com/business/2016/feb/02/talktalk-cyber-attack-costs-customers-leave. [Accessed: 15-Nov-2018].

[71] Google, ‘A new approach to China,’ 2010. [Online]. Available: https://googleblog.blogspot.com/2010/01/new-approach-to-china.html. [Accessed: 12-Nov-2018].

[72] C. Graham, ‘NHS cyber-attack: Everything you need to know about ‘biggest ransomware’

offensive in history,' 2017. .

[73] K. Kwang, 'Singapore health system hit by 'most serious breach of personal data' in cyber-attack; PM Lee's data targeted,' 2018. [Online]. Available: https://www.channelnewsasia.com/news/singapore/singhealth-health-system-hit-serious-cyber-attack-pm-lee-target-10548318. [Accessed: 13-Dec-2018].

[74] Agence France-Presse, 'Cathay Pacific hit by data leak affecting up to 9.4m passengers,' 2018. [Online]. Available: https://www.theguardian.com/technology/2018/oct/24/cathay-pacific-hit-by-data-leak-affecting-up-to-94m-passengers. [Accessed: 09-Apr-2019].

[75] H. Kuchler, 'Uber to beef up security team in push to strengthen data safety,' 2015. [Online]. Available: https://www.cnbc.com/2015/08/17/uber-strengthens-security-team-to-allay-data-safety-hack-worries.html. [Accessed: 12-Dec-2018].

[76] S. Larson, 'Uber's massive hack: What we know,' 2017. .

[77] Local Government Council, 'Copeland Borough Council: managing a cyber-attack,' 2018. [Online]. Available: https://www.local.gov.uk/copeland-borough-council-managing-cyber-attack. [Accessed: 02-Oct-2018].

[78] J. McCrank, J. Finkle, 'Equifax breach could be most costly in corporate history,' 2018. [Online]. Available: https://uk.reuters.com/article/us-equifax-cyber/equifax-breach-could-be-most-costly-in-corporate-history-idUKKCN1GE257. [Accessed: 22-Nov-2018].

[79] N. A. Office, 'Investigation: WannaCry cyber-attack and the NHS,' 2017. [Online]. Available: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs. [Accessed: 03-Oct-2018].

[80] E. Palmer, 'Merck has hardened its defenses against cyber-attacks like the one last year that cost it nearly $1B,' 2018. [Online]. Available: https://www.fiercepharma.com/manufacturing/merck-has-hardened-its-defenses-against-cyber-attacks-like-one-last-year-cost-it. [Accessed: 23-Nov-2019].

[81] J. Park, K., Hong, 'Millions of passengers hit in worst ever airline data hack,' 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-10-25/cathay-pacific-reports-data-breach-affecting-9-4-million-fliers. [Accessed: 29-Nov-2018].

[82] B. Pierson, 'Anthem to pay record $115 million to settle U.S. lawsuits over data breach,' 2017. [Online]. Available: https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML. [Accessed: 02-Dec-2018].

[83] Reuters, 'Dubai's Careem hit by cyber-attack affecting 14 million users,' 2018. [Online]. Available: https://www.reuters.com/article/us-careem-cyber-attack/dubais-careem-hit-by-cyber-attack-affecting-14-million-users-idUSKBN1HU1WJ. [Accessed: 09-Apr-2019].

[84] AJC, 'Cost of City of Atlanta's cyber attack: $2.7 million — and rising,' 2018. [Online]. Available: https://www.ajc.com/news/cost-city-atlanta-cyber-attack-million-and-rising/nABZ3K1AXQYvY0vxqfO1FI/. [Accessed: 09-Apr-2019].

[85] Reuters, 'Singapore cyber attack has hallmarks of state-linked group, government says,' 2018. [Online]. Available: https://www.reuters.com/article/us-singapore-cyber-attack/singapore-cyber-attack-has-hallmarks-of-state-linked-group-government-says-idUSKBN1KR0YR. [Accessed: 13-Dec-2018].

[86] Seatrade Maritime News, 'Maersk Line introduces new cyber security measures following Petya attack,' 2019. [Online]. Available: http://www.seatrade-maritime.com/news/europe/maersk-line-

introduces-new-cyber-security-measures-following-petya-attack.html. [Accessed: 21-Nov-2018].

[87] Skynews, ‘Equifax fined £500,000 for failing to protect customer details in cyber attack,’ 2018. [Online]. Available: https://news.sky.com/story/equifax-fined-500000-for-failing-to-protect-customer-details-in-cyber-attack-11502809. [Accessed: 23-Nov-2018].

[88] N. Statt, ‘Uber covered up a cyber-attack last year that exposed data of 57 million riders and drivers,’ 2017. [Online]. Available: https://www.theverge.com/2017/11/21/16687796/uber-cyber-attack-data-breach-exposed-users-57-million. [Accessed: 03-Nov-2018].

[89] The Telegraph, ‘Private data of 500 million Marriott guests exposed in massive breach,’ 2018. [Online]. Available: https://www.telegraph.co.uk/technology/2018/11/30/private-data-500-million-marriott-guests-exposed-massive-breach/. [Accessed: 13-Oct-2018].

[90] The Telegraph, ‘British Airways hacking: Customers cancel credit cards as airline defends handling of ‘sophisticated’ cyber attac,’ 2019. [Online]. Available: https://www.telegraph.co.uk/news/2018/09/07/british-airways-hacking-customers-cancel-credit-cards-airline/. [Accessed: 02-Oct-2018].

[91] K. Zetter, ‘Google hack attack was ultra-sophisticated, new details show,’ 2010. [Online]. Available: https://www.wired.com/2010/01/operation-aurora/. [Accessed: 15-Nov-2018].

[92] BBC News, ‘The Interview: A guide to the cyber-attack on Hollywood,’ 2014. .

[93] BBC News, ‘Council hit by cyber attack reveals £2m cost,’ 2018. [Online]. Available: https://www.bbc.co.uk/news/uk-england-cumbria-45811509. [Accessed: 29-Oct-2018].

[94] Buchanan E., ‘China carried out cyber attacks on Google,’ *BBC News*, 2010. [Online]. Available: https://www.bbc.co.uk/news/uk-england-london-45440850. [Accessed: 24-Nov-2018].

[95] Birnbaum E., ‘Marriott looking at China in data breach: report,’ 2018. [Online]. Available: https://thehill.com/policy/cybersecurity/420136-marriott-looking-at-china-in-data-breach-report. [Accessed: 12-Oct-2018].

[96] Careem, ‘Important security information,’ 2018. [Online]. Available: https://blog.careem.com/en/security/. [Accessed: 15-Oct-2018].

[97] A. Cuthberson, ‘North Korean hackers linked to Sony Pictures attack have servers seized in Thailand,’ 2018. [Online]. Available: https://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-hackers-server-thailand-sony-pictures-cyber-attack-a8329586.html. [Accessed: 12-Dec-2018].

APPENDIX I
SUMMARY OF CASE CYBER SECURITY

Organization	Nature of cyber-attacks in brief	Effects of the attacks	Organizational responses: Tactical response (TR) and strategic response (SR)	Stages Reflected in Case
Multinational companies				
China Google	In 2010, cyber-attackers hacked into Google China's Office Systems and retrieved Google's system codes. According to McAfee, the attackers used about 12 different malwares and several levels of encryption to ransack the company's networks. Further investigations revealed that some Gmail accounts had also been compromised. Google suspected that the Chinese government was behind the attack as part of its attempt to monitor conversations of human rights activists.	While its aims were unsuccessful, the attack led to a hostile relationship between Google and China with the multinational refusing to censor its reports according to Chinese guidelines. Google noted after the attack that	TR: In March 2010, Google relocated its google.cn servers to Hong Kong in order to escape China's Internet filtering policy. SR: In response to the attack, the multinational built more efficient infrastructure and architecture to enhance security of its systems. Google also initiated a worldwide educational campaign for its users, informing them on ways to protect themselves from attacks, through for instance, using proper antivirus programs.	Step 2, Step 3
Maersk	In June 2017 cyber-attackers prevented Maersk employees from accessing their data, unless they made a ransom payment of $300 in Bitcoin. The attack affected Maersk Line, APM Terminals and Damco, all business units of Maersk. Researchers suspected that the attack was led by Russia's against Ukranian Organisations.	The attack led the organisations' container ships and all 76 of its port terminals to cease operations and resulted in a decline of 250 million to 300 million in profits. 'It was frankly quite a shocking experience…Your email goes down, all your address system. We ended up having to use WhatsApp on our private phones'. (Seron Skuo, 2017. Quoted from FT).	TR: According to Møller-Maersk chair, Jim Hagemann Snabe, Notpetya's destructiveness required an urgent installation of 4000 new servers, 45,000 new PCs and 2,500 applications. SR: According to the CEO, it is not possible to completely prevent a future attack. Notwithstanding, the organisation reviewed its systems to become more resilient by introducing new measures for the future in order to 'isolate an attack quicker and restore systems quicker'. According to Maersk (2017), 'In response to this new type of malware, we have put in place different and further protective measures'.	Step 1, Step 2, Step 3
Sony Pictures, US	Sony pictures faced a massive cyber-attack, Wannacry, in October 2014. The attackers accessed and shared yet-to-be released movies on illegal sites and stole confidential information belonging to Sony Pictures and individual employees, which they then circulated online. Investigations reveal that Lazarus, a group with links to the North Korean Government may have been behind the attacks with the aim of stopping Sony Pictures from airing 'The Interview', a satirical comedy movie around an assassination plot of the North Korean leader.	Employees could not use their computers for more than six weeks after the attack for fear of remnants of the attack. Various confidential information belonging to Sony Pictures and individual employees were made public. Employees of Sony levelled about seven class action lawsuits against their employer for not taking strict steps to protect their confidential information. Theatres were unable to show 'The Interview' on scheduled dates due to threats from the attackers made terrorist threats against cinemas showing the film.	TR: Sony provided security and protection to top producers and actors linked to the movie, The Interview. It also offered a year of credit monitoring to current employees. Sony's legal partners asked all media houses to stop downloading information that had been compromised and also demanded that they destroy any data they already had in their possession. Using the services of third-party companies, like Entura International, Sony Pictures tried to block distribution of the stolen data and to delete all links that led to the hacked information. SR: At the national level, the United States Government issued a legislative proposal to update and establish new laws that empowered the country to prosecute crimes related to cybercrime and at the same time uphold the privacy of Americans.	Step 2, Step 3
Liberty Holdings, South African Insurance Company	The company was the victim of a cyber-attack in June 2018, in which confidential information of top clients were retrieved. The company only got to know of the attack when the attackers informed it that it had	Liberty Holdings' Shares fell by nearly 5% after the cyber-attack.	TR: Relevant authorities in South Africa, as well as clients were informed of the attack. There was an immediate investigation into Liberty Holding's Systems to identify vulnerable aspects of the IT Infrastructure Systems. The organisation then secured computer systems	Step 2, Step 3

Organization	Nature of cyber-attacks in brief	Effects of the attacks	Organizational responses: Tactical response (TR) and strategic response (SR)	Stages Reflected in Case
	accessed and retrieved data, which will be shared with the public if they were not compensated. The Insurer, however, did not make this payment.		**SR:** According to the Insurer, measures have been put in place to secure computer systems and ensure that individual information is protected. The details of these are not yet publicly available.	
NHS, England	In 2017, NHS, England faced one of its greatest cyber-attacks in recent times. The attack, WannaCry, encrypted data on infected computers and made it impossible for users to access their files. The attackers, Shadow Brokers, suspected to be linked to Russia, then demanded a ransom, which the NHS refused to honour in line with legal requirements. According to the Telegraph, this attack successfully executed when emails sent by the attackers are mistakenly opened on any of their target's computers, leading to phishing. Once the attackers have access to the target's systems, they make it impossible for users to access any files.	34% of NHS Trusts worldwide faced severe disruptions to services. 6, 912 appointments were cancelled although there were expectations that a higher number of about 19000 unrecorded appointments may have been cancelled altogether. Huge costs in the form of cancelled appointments, restoration of data systems and additional support from local NHS bodies were incurred.	TR: Patients from some Trusts, including London, Essex, Hertfordshire, Hampshire and Cumbria were transferred to other Accident and Emergency departments, while two other Trusts were reinforced with external support. A cyber security researcher's work helped to recover systems and stop the spread of the malware. SR: NHS England and NHS Improvement announced to all major health institutions instructing them to implement all alerts issued by NHS Digital between March and May 2017. They were also asked to ensure that all local firewalls have been secured. NHS England also drew a contract with Microsoft, to provide a new package that would help identify threats early and contain malicious attacks without spreading to other places. According to the Health Secretary, 'We have been building the capability of NHS systems over a number of years, but there is always more to do to future-proof our NHS against this threat…This new technology will ensure the NHS can use the latest and most resilient software available – something the public rightly expect' (Jeremy Hunt, Health Secretary). In addition, all healthcare organizations have now been required to meet 10 standards set for data security and protection toolkit. Lord O'Shaughnessy (2018), a health minister, said in light of this: 'Patient data must be properly protected and this significant investment will help to keep our systems resilient and up to date'.	Step 1, Step 2, Step 3
TalkTalk, Internet Service Provider, UK	In 2015, over 150 000 of TalkTalk's customers' data were compromised when 'a significant and sustained' cyber-attack was carried out on its website. Investigations on the attack revealed that the stolen data had not been encrypted, making it an easy target for the attackers. The information retrieved from customers included credit card and bank account details. In November 2018, two young men, Matthew Henley and Connor Allsop both from Tamworth, England, were jailed for their involvement in the attack.	As a result of the attack, 101000 customers switched from TalkTalk to other service providers. Numbers of new customers dropped significantly and online sales operations reduced to the barest minimum. The company was also fined £400,000 by the Information Commissioners' Office for not taking basic steps to prevent the attack.	TR: TalkTalk offered free upgrades to customers to discourage them from switching to competitors. They also invited an independent, external party be to assess all its processes and security systems in order to identify areas of vulnerabilities. SR: TalkTalk announced that it had invested more in security of its cyber systems. In addition, the organisation reported that cyber security had been integrated into the whole organization, rather than as a separate business function. 'Security is discussed at every meeting and is embedded in everything we do with the products and the services that we launch and has become part of the day to day discussion…we currently have an online training system with all our staff going through training programmes making sure employees are aware of all the types of security and risk and what we would expect in terms of a secure approach…' (Duncan Gooding, COO, TalkTalk).	Step 1, Step 2, Step 3

Organization	Nature of cyber-attacks in brief	Effects of the attacks	Organizational responses: Tactical response (TR) and strategic response (SR)	Stages Reflected in Case
			However, quite recently in March 2018, Sky news reported a warning from an attacker who pointed out key vulnerabilities in TalkTalk's website, which seems to question the effectiveness of the strategies the organization has put in place since the attack.	
Carphone Warehouse	In 2015, cyber-attackers targeted Carphone Warehouse, stealing data from about three million customers and 1000 employees. The company's onestopphoneshop.com, e2save.com and mobiles.co.uk websites were the business units affected in the attack. According to the Financial Times, the attackers capitalized on an outdated WordPress interface, which was still being used at Carphone Warehouse.	5.9 million payment card details and 1.2 million personal data records including names, addresses and email details were stolen. This meant that affected customers and employees were vulnerable to possible fraud. Carphone was fined an amount of £400, 000 by the Information Commissioners Office and shares fell about 6.4%. ICO fined Carphone for failing in its duty to carry out measures that would protect the security of stakeholders online. According to the UK Information Commissioner, Elizabeth Denham, said, 'A company as large, well-resourced and established as Carphone Warehouse, should have been actively assessing its data security systems and ensuring systems were robust and not vulnerable to such attacks.'	TR: The company informed all affected people, relevant card companies and national security agencies of the attack. SR: The company said it had invited cyber experts and enhanced its security to fight against future attempts.	Step 1, Step 2
Anthem Insurers	Anthem was affected by a cyber-attack in 2015 that leaked personal information of about 75 million customers, employees and the CEO, Joseph R. Swedish. The attacker seemed to have gained access to and retrieved data relating to names, date of births, addresses and social security numbers. The organisation's investigations revealed that data had been stolen for some weeks before it was discovered.	The organization was charged a total amount of $115 million for exposing peoples' data. Stolen data could lead to irreparable problems, such as identity theft.	TR: The company offered two years-worth of credit monitoring to its customers and advised them to monitor their accounts. The Cyber Security firm, Mandiant, also assessed and evaluated all their security systems. In addition to these, the company contacted relevant law enforcement and security agencies, including the FBI about the attack.	Step 1
Merck and Co, U.S. Drug maker	In 2017, Merck was one of the victims of the Notpeya cyber-attack. Notpeyers affected organizations which did not have a security patch in its Microsoft Systems. The attack affected three units: operations, manufacturing, research and sales, significantly disrupting operations in these areas. Employees found a ransomware message on their computers. According to an anonymised employee report on the Wasington Post: 'Some people looked like they had their hardware wiped — it just shut down the whole network site,'	It took at least six months to restore most systems. There were severe disruptions on global operations and new drugs could not be produced. Merck had to rely on the US government for certain supplies in order to meet demand. In addition, the attack led to a loss of $260 million in sales and had to use $360 for additional marketing of its products.	TR: Employees were officially informed of the attack through a public address system. Due to the inaccessibility of computer systems, they were also asked to call a number, which is often used during severe weather emergencies to check if they had to come to work the next day.	Step 2
Cathay Pacific Airlines	In October 2018, Cathay Pacific was the victim of a cyber-attack that leaked personal information, such as names, identity card numbers, passport details, email addresses	There was a significant drop in shares, with a decline of $ 201 million in market value. Customer data were exposed, although it appears no fraud activities had been carried out.	TR: The focus of the first three months of the attack was an attempt to contain the attack. All affected customers were informed and offered guidance on how to protect themselves, including an option for complementary monitoring for all passengers. A dedicated	Step 1, Step 2, Step 3

Organization	Nature of cyber-attacks in brief	Effects of the attacks	Organizational responses: Tactical response (TR) and strategic response (SR)	Stages Reflected in Case
	and credit card details of about 9.4 million passengers. The attack was spotted during an IT operation the organisation was carrying out. However, it appears the breach had been going on for much longer. According to Cathay Pacific, even during the period after they had first spotted the attack and started making attempts to investigate and stop it spreading, they continued to be attacked for over 3 months, between March and May.		website was also set up for customers to communicate with the organisation on their concerns. In addition, they informed relevant security agencies and started an investigation into the attack. The Airline also said that it had spent over $128 million on IT systems and security in the 3 years leading to the attack and would continue to do so. In a video placed on their website, CEO, Rupert Bogg confirmed these strategic activities 'Upon discovery, we acted immediately to contain the event and to thoroughly investigate,' Hogg said. 'We engaged one of the world's leading cybersecurity firms to assist us and we further strengthened our IT security systems too.' (CEO Rupert Bogg.'	
Singapore Health Sector	In 2018, Singapore's largest healthcare provider, SingHealth, was attacked by cyber-security experts. According to the government, the attack was led by an 'Advanced Persistent Threat' group, which is often linked to a state. The attack leaked information of 1.5 million patients, including information on the President. The aim of the attack was unclear. According to the Prime Minister, Lee Hsien Loong, 'I don't know what the attackers were hoping to find. Perhaps they were hunting for some dark state secret, or at least something to embarrass me (The Telegraph, 2018)'	Personal non-medical data of 1.5 million patients were compromised. This included patient's names, addresses birthdates and information on identity cards were accessed and retrieved by the attackers from patients who visited various health care centres from May, 2015 to July, 2016.	TR: All patients were contacted and informed about the data breach and specifically whether their data had been affected. SR: Measures were taken to improve security of IT systems. This included Internet Separation policies. In addition, more controls were introduced. All user and system account were reset, while more measures were put in place to enhance monitoring. Drawing on external expertise, the IHiS also assessed the public healthcare systems to evaluate cybersecurity policies, threat management processes, IT system controls and organisational and staff capabilities. Another measure taken was to educate both public and private healthcare institutions on ways of protecting themselves against cyber-attacks. Regardless of these efforts, the Minister of Health noted that attackers seemed to be a step ahead of techniques of destruction. 'We will do our utmost to secure our IT systems. However, unfortunately, we cannot completely eliminate the risk of another cybersecurity attack,'	Step 1, Step 2, Step 3
Equifax. Consumer credit recording company. UK	In 2017, the parent company of Equifax, located in US faced a cyber-attack. This affected a file containing 15.2 million UK records stored between 2011 and 2016. The file contained data on customers, as well as duplicates of data for trials.	The effects of the attack on customers were classified into four categories. The first group of costumers had the emails linked to their Equifax accounts accessed. The second group had log in details of their Equifax account, including names, passwords, secret question and answers. The third category of customers had their driving licence number accessed. The fourth group had their phone number accessed. The organisation was fined an amount of £500,000 for failing to protect customers' interests. According to The Information Commissioner's Office (ICO), this was because of vulnerabilities in Aquifax' system which prevented them from engaging. 'The Information Commissioner's Office (ICO) found that Equifax's systems to manage the personal information were inadequate and ineffective, while investigators found significant	TR: All affected customers were contacted and informed of the level of damage or category of risk they fell into. They were also informed of free ID protection offered by Equifax. In terms of costs, Equifax recently reported that it had USD 125 million of cyber security insurance, which it would use to defray some of the cost of the attack.	Step 2

Organization	Nature of cyber-attacks in brief	Effects of the attacks	Organizational responses: Tactical response (TR) and strategic response (SR)	Stages Reflected in Case
		problems with data retention, IT system patching and audit procedures'. Reuters (2017) estimated a cost of about $600 million which the company spent on legal fees, free protection form identity theft for customers and upgrades to technology and security systems.		
British Airways	In August 2018, British Airways was the target of a cyber-attack, where customers who had booked a flight between August 21st and 5th September had their personal data accessed. According to Sky news reports, The number of customers in this bracket were about 400, 000. According to BA's chairman, Alex Cruz, while the hackers did not access any encrypted data, they used illicit ways to access the organizations website and retrieve customers' bank details used to make flight payments.	Many customers had to cancel their credit cards and request replacement cards. This was to prevent the hackers from using the information they had collected, which included card details, from making payments. Based on new penalties under the GDPR regulations, BA is expected to be fined about £500 million.	TR: After BA realised the data breach, they informed all affected customers. The organisation also promised financial compensation for any customers who had incurred any financial lost from the hackers' activities.	Step 2
Uber, ride sharing company	Hackers broke into Uber's GitHub account and stole information, relating to names, email addresses, phone numbers and drivers' license numbers, from about 57 million customers and drivers in 2016. According to the CEO, the hackers used a third part cloud-based service to carry out the attack. The organisation was criticised for not disclosing the attack for almost a year after it happened. Instead, it paid hackers $100,000 to destroy all data they had accessed.	Aside the customer and drivers' data that were compromised, Uber also came up wide criticisms provoked by a Blomberg report, which rebuked the organisation for refusing to disclose the attack. The Chief Security Officer and some of his subordinates who led decisions to be silent on the attack were sacked from the organisation. Uber faced a number of lawsuits from state and local governments for trying to conceal legal information and not protecting customer data.	TR: Uber paid an initial $100,000 to the attackers to destroy the data they had stolen. This was against regulations that all data breaches be reported to law enforcement agencies and to avoid paying ransom to hackers. In response to the attack in particular, the CEO claimed that it 'took immediate steps to secure the data and shut down further unauthorized access by the individuals. We also implemented security measures to restrict access to and strengthen controls on our cloud-based storage accounts,' SR: As at 2017, Uber had planned to invest in drastically improving security and specifically protecting their systems against further hack attempts. It was expected that about 75 more employees would be recruited to support the work of the security team. In addition, the organisation made significant progress by recruiting a new Chief Security Officer, Joe Sullivan, who was previously a federal prosecutor of cyber-crime. He promised to leverage on technology to improve cyber security as well as security against physical threats, trust and safety of customers. The new CSO also noted plans to monitor the use of data even by employees of Uber across the world in order to prevent abuse of customers' data. As he noted, 'Every company is a data company now, no one can be unsophisticated. The challenge is half the company needs access to customer data some of the time — it is not just customer support, it is marketing, engineers as they iterate, communications when they need to figure out what happened in an incident'. In response to the problem this poses, the organisation now runs random data auditing to ensure that employees are only accessing data when necessary and for its intended purposes.	Step 1, Step 2, Step 3

Organization	Nature of cyber-attacks in brief	Effects of the attacks	Organizational responses: Tactical response (TR) and strategic response (SR)	Stages Reflected in Case
Marriott Hotel, Global Hotel Chain	In November 2018, Marriott Hotel reported that data of about 500 million customers who had used its Starwood Hotels, had been unlawfully accessed by cyber attackers. The attackers hacked into Starwood's Room Reservations Network, used by Sheraton and retrieved customers' home addresses, emails, credit card details, dates of birth and passport details. According to the Multinational, although its internal security tool had only spotted the attack in September 2018, it appears to have been going on for four years, making it not only the second largest attack in terms of number of customers affected, but also one of the most persistent attacks on a single organisation in recent times. According to cyber security experts, Marriott may have become vulnerable after it acquired Starwood Hotels in 2016, given that the latter was already experiencing hacks in its system. Investigations suggest that Chinese Hackers may be behind the attack.	Marriott was faced with severe backlash from customers who complained that Marriott had delayed informing them about the breach, leaving them to find out about it in media reports. The immediate effect on Marriott Hotel was a drop in share price by 5% the next morning after the announcement of the attack. While still ongoing, it is expected that the organisation will pay a colossal sum of money in legal fees.	TR: In line with legal requirements, Marriott reported the attack to UK'S Information Commissioners' Office (ICO), who noted that they had started investigations into the breach Marriott also set up a website where they provided customers guidance on what they could do if they had been affected (info.starwoodhotels.com) (and put up call centers to specifically respond to customers whose data had been compromised. They also tried removing all traces of encrypted information that the attackers had done. In addition to these, Marriott provided customers in three regions, UK, Canada and US a year-long subscription to Webwatcher, which helps to detect frauds. SR: On their website, Marriott noted the following as steps they were taking to reduce possibilities of future recurrence 1. Engaging leading security experts to help determine what occurred. 2. Installed additional security tools to help gather facts 3. Leveraged both internal and external security teams to work nonstop in investigating the incident On a general level, they reported that 'We are supporting the efforts of law enforcement and working with leading security experts to improve. Marriott is also devoting the resources necessary to phase out Starwood systems and accelerate the ongoing security enhancements to our network'.	Step 2, Step 3
Instagram, Social Media Platform [62], [63]	In August 2018, Instagram users had their account details, including profile images, handles, contact details and bios had been changed. The attackers replaced all profile photos with still photos from Disney movies and replaced email addresses with ones ending with .ru, a Russian domain. While the organisation's investigations found that most of the hacked accounts were not two-factor secured, it was also found that some users' who had done the two-factor authentication were still affected.	A number of uses reported not being able to access their accounts. Private data of celebrities and ordinary users were stolen. In fact, the hackers sent a sample of stolen data to the Daily Beast, perhaps, as prove of their attack.	TR: A number of instructions were sent out to Instagram users to guide them on securing their data against attacks. This included directions to develop stronger and more secure passwords and to ensure that they did a two-factor authentication. Users were also informed to 'report any unusual activity through our reporting tools. According to Instagram, they also fixed the bug immediately they found out about it and cooperated with law enforcement.	Step 2
Careem (A Dubai Ride Hailing App operating in Mena, Pakistan and Turkey)	Information from about 14 million customers and drivers of Careem across 13 countries were stolen. This included ride histories, names, phone numbers, credit card details and email addresses. Careem got to know about the attack based on a note the attacker left on their system. In an apology email to customers, the company said 'We regularly review and update our security systems – this time it	According to Forbes (2018), the main impact of this attack is the erosion of trust by customers that Careem and all other online based transactions are likely to confront. This is especially so because the Middle East is still emerging in the use of online transactions and customers may be discouraged on the security of their systems.	TR: The organisation informed law enforcement agencies of the attack and worked with Interpol to investigate the incident. SR: The company has since the attack reported huge investments into cybersecurity, including hiring the expertise of leading cyber security personnel. 'As soon as we detected the breach, we launched a thorough investigation and engaged leading cybersecurity experts to assist us in strengthening our security systems. We are also working with law enforcement agencies. Throughout the incident, our priority has been to protect the data and privacy of our customers and captains. Since discovering the issue, we have worked to	Step 2

Organization	Nature of cyber-attacks in brief	Effects of the attacks	Organizational responses: Tactical response (TR) and strategic response (SR)	Stages Reflected in Case
	wasn't enough to prevent an attack,' (Careem Official Blog, 2018).		understand what happened, who was affected and what we needed to do to strengthen our network defences,' (Careem Official Blog Post, 2018)	
Non-profits, NGOs, charities, community trusts and foundations				
Copeland Council	In August 2017, the Copeland Council was the victim of a cyber-attack, which cost the government organization about 2 million pounds. According to reports, core services of the council, including pay rolling, planning and environmental health, had to be stalled. While no sensitive data was stolen, the attackers demanded ransoms, in the form of Bitcoins or refuse access to the organizations' files.	The attack cost the organization about 2m pounds. Employees lost substantial data running into several years' worth of work. It slowed down key activities given that basic IT functions including printing and accessing files were not available. Most of the problems were not resolved for at least 10 weeks after the attack. Describing the effect of the attack, the council explained on the Local Government Webpage how '*no-one* in Copeland had *any* access to any files or systems that were saved on shared or personal drives. The only accessible files were those stored on individual devices and those saved on Microsoft OneDrive' (Local Government Association, 2018). This meant that the payroll department for instance could not generate financial systems at all.	TR: An IT team was set up, led by the organization's IT Manager. The team also included experts from neighboring organizations and partners as well as the cyber security sector. The police cyber-crime unit and Information Commissioners' Office were informed. SR: Copeland Council has invested efforts in enhancing its resilience against cyber-attacks. This includes running a comprehensive health check for its cyber systems and carried out extensive cyber training for all staff and members. Teams now rely on cloud storage to prevent sudden loss or access problems caused by potential future attacks. In addition, the council has purchased more updated IT equipment and restructured the internal networks to create a sort of protection from the effects of future attacks. In addition, roles and responsibilities were redesigned to enhance accountability. As explained by the CEO of the council, Ms Graham 'There is no way we could have kept this attack out, but had we had great IT investment we probably would have recovered quicker.'	Step 2, Step 3
South Korea	In March 2013, cyber attackers used a malware called DarkSeoul, to carry out attacks against various institutions and online systems in South Korea including the three largest television stations, a bank, ATM machines and mobile payments. Based on previous evidence of attacks by North Korea, South Korea blamed this particular attack on North Korea.	A large number of banking files went missing. Some internet banking services became completely unresponsive and computer systems of the television stations stopped working.	TR: A security alert was raised by the military. In addition, the Korea Communications Commission asked government agencies and businesses to increase the possible number of monitors to guard against any potential attacks. SR: Since the attack, cyber-security has become one of the core policy areas of the South Korean Government. They have particularly invested in sophisticated ways of monitoring systems to spot any prevent future attempts of cyber-crimes.	Step 2, Step 3
Edinburg City Council	Email addresses of about 13,000 people in Edinburg were stolen in an attack that affected the Council's systems. According to investigations, this happened when their website service provider's systems were hacked by cyber-attackers.	In a report by the Council, the email addresses, which were stolen were noted to have led to loss of data integrity, abuse of confidentiality and a poor reputation	TR: The Council informed all affected clients of the attack and asked them to change existing passwords they had previously used to access the council's web services. They also provided a number and website where all who had been affected could share their concerns. The UK Information Commission, as well as the Government's Computer Emergency Support Team were informed. SR: In the 2016 Audited Annual Accounts, the Council listed the following controls to improve cyber-security 1. Encrypt all laptops and media. 2. Carry out education on data awareness 3. Put in place service automation 4. Ensure that leavers from the council are prevented from accessing the Council's IT	Step 1, Step 2, Step 3
City of Atlanta, US	In March 2018, Atlanta City in the US was affected by a cyber-attack that infiltrated the bulk of the municipal's systems. The	First, about 424 software by the city could not operate online. Residents could not undertake	TR: The Council worked closely with the FBI and other relevant security agencies to investigate the attack. They also employed Secureworks, a cyber-security firm to support the investigations.	

Organization	Nature of cyber-attacks in brief	Effects of the attacks	Organizational responses: Tactical response (TR) and strategic response (SR)	Stages Reflected in Case
	attackers demanded a ransom payment of approximately $50,000 in bitcoin. The attack has been blamed on the cybercrime group, SanSam, which has been involved in various attacks.	basic public tasks that relied on the City's systems, such as paying for parking tickets and utility bills. Key information across the City's public services, including legal documents dating back to almost 10 years were lost. It took 5 days for employees to be able to access their computers, slowing down work and the council's ability to offer core services, including courts and police to clients. In fact, it took longer for some employees to regain access to the system. The Council spent $2.7 million in emergency contracts.	Employees were asked not to power on any government computers. The Council deployed a number of contractors as an emergency measure to recover its activities. It also undertook software upgrades and had plans of buying new gadgets including laptops, mobile phones and tablets.	

Synthesized from: [57], [62]–[97]