Computers & Security 135 (2023) 103525

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Moving towards agile cybersecurity incident response: A case study exploring the enabling role of big data analytics-embedded dynamic capabilities

Ayesha Naseer [a], Humza Naseer [b], Atif Ahmad [c,*], Sean B Maynard [c], Adil Masood Siddiqui [d]

[a] Department of Computer Software Engineering, National University of Sciences and Technology, Islamabad, Pakistan
[b] School of Accounting, Information Systems and Supply Chain, College of Business and Law, RMIT University, Melbourne, Australia
[c] School of Computing and Information Systems, Faculty of Engineering and IT, University of Melbourne, Melbourne, Australia
[d] Department of Electrical Engineering, National University of Sciences and Technology, Islamabad, Pakistan

ARTICLE INFO

Keywords:
Cybersecurity
Incident response
Big data analytics
Dynamic capabilities
Agility

ABSTRACT

Organizations are at risk of cyber-attacks more than ever before due to the ongoing digitalization of business operations. Industry reports indicate that it is not a matter of if but when organizations become victims of cyber-attacks or breaches. In this research, we argue that organizations must enable *agility* in their incident response (IR) to quickly respond to diverse cybersecurity threats, and big data analytics (BDA) plays a pivotal role in enabling agility in the IR. Drawing from dynamic capabilities theory, we conducted a field study using a case study approach to examine the following research question: *What dimensions of big data analytics-embedded dynamic capabilities enable agility in cybersecurity incident response?* We develop a framework that presents five key dimensions of BDA-embedded dynamic capabilities (*data consolidation, threat intelligence, incident investigation, analytical skillset, and cybersecurity analytics warehouse*) in IR at four specific stages, that is, manual analysis, basic analytics, advanced analytics, and pervasive analytics. The detail of the framework explains how BDA-embedded dynamic capabilities at the pervasive analytics stage enable agility in IR by infusing agile characteristics of *flexibility, speed*, and *learning* in IR. This study contributes to the knowledge of IT-embedded dynamic capabilities and cybersecurity IR agility. Detailed recommendations are also provided for potential practitioners.

1. Introduction

The growing digitization and automation of business operations are putting organizations at risk of cyber-attacks more than ever before (Kavanagh et al., 2021; Yeoh et al., 2022). Organizations are now starting to consider cybersecurity a significant business risk because a successful cyber-attack can cause major damage to organizations in terms of financial loss, reputational damage, and legal liabilities (He et al., 2022; Kotsias et al., 2022). As a consequence, organizations are now continuously looking for approaches to improve their cybersecurity incident detection and response processes (Khan et al., 2021; McMillan and Proctor, 2018).

The cybersecurity incident response (IR) process consists of a collection of procedures aimed at identifying, investigating, and responding to potential security incidents in a manner that minimizes impact and supports rapid recovery (Creasy and Glover, 2013; Kotsias et al., 2022). We argue that for the IR process to be effective in dealing with unknown, complex, and sophisticated cyber threats, its underlying activities (detection, containment, eradication, and recovery) must be performed in an agile manner (Grispos et al., 2017; Naseer et al., 2023). This requires IR teams to have skills, tools, and processes that enable the enterprise-wide collection, integration, and analysis of all relevant data related to cybersecurity incidents to make informed decisions in a timely manner.

Big data analytics (BDA) is an organizational capability that helps in the collection, integration, and analysis of a large amount of business data generated in various forms at high speed to gain business insights for informed decision-making (Grover et al., 2018; Mikalef and Krogstie, 2020). Prior research has examined the role of BDA as an enabler of dynamic capabilities (i.e., "*the ability to integrate, build, and reconfigure internal and external competencies to address rapidly changing environments*" (Steininger et al., 2022; Teece et al., 1997). For example, Conboy

* Corresponding author.
E-mail address: atif@unimelb.edu.au (A. Ahmad).

https://doi.org/10.1016/j.cose.2023.103525
Received 19 October 2022; Received in revised form 29 September 2023; Accepted 2 October 2023
Available online 7 October 2023

et al. (2020) showcase how BDA characteristics (volume, velocity, variety, variability, veracity, and visualization) can be leveraged to enable dynamic capabilities in the field of operations research. In particular, a critical enabler of processes underpinning dynamic capabilities is argued to be the data itself (Mikalef et al., 2021). By making use of BDA to collect, integrate and analyze cybersecurity data from a variety of sources such as logs, networks, endpoints, sensors, and cloud systems, cybersecurity managers can discover useful information about cybersecurity incidents (Naseer et al., 2021b; Eastman and Versace, 2015). While the ability of BDA to improve cybersecurity and enable dynamic capabilities, in general, has gained much attention in both research and practitioner domains, research on the transformative effects of BDA-embedded dynamic capabilities on the agility of cybersecurity IR is limited. This gap in the literature motivated our study's key research question: *What dimensions of big data analytics-enabled dynamic capabilities enable agility in cybersecurity incident response?*

To address this question, we conducted an in-depth case study on the IR function of a multinational financial organization as it used BDA to make sense of and respond to cybersecurity incidents. Integrating insights from the empirical data with existing literature on cybersecurity IR, BDA, and dynamic capabilities theory, we propose a framework that identifies five key dimensions of BDA-embedded capabilities (data consolidation, threat intelligence, incident investigation, analytical skillset, and cybersecurity analytics warehouse) in IR at four specific stages, that is, manual analysis, basic analytics, advanced analytics, and pervasive analytics. The details of the framework explain how the utilization of BDA-embedded dynamic capabilities at the pervasive analytics stage enables agility in IR by infusing agile characteristics of *flexibility, speed,* and *learning* in IR.

In the following sections, first, we provide a review of the relevant literature. Next, in the research methodology section, we describe the case study and elaborate on the method of data collection and analysis. We then describe an illustrative story to explain the results of the fieldwork. Next in the discussion section, we explain our research's theoretical contributions and practical implications. Finally, we conclude the paper by providing the limitations of our study and directions for future research.

2. Literature review

In this section, we review the literature on the intersection of cybersecurity, IR, BDA, and dynamic capabilities. In addition, we also unpack the concept of agility in cybersecurity IR.

2.1. Overview of cybersecurity and IR

Cybersecurity is the practice and actions associated with security risk management processes followed by organizations and aims to protect the confidentiality, integrity, and availability of an organization's digital assets (Adesemowo, 2021; von Solms and van Niekerk, 2013). In the context of this study, we define a digital asset as any digital material owned by an organization or individual that is uniquely identifiable and can be used to realize value.[1] For example, data, systems, digital technologies, documents, audio, videos, websites, and information. Cybersecurity is important because an organization's digital assets are valuable and at the same time are vulnerable to cyber-attacks (Kavanagh et al., 2021; Wong et al., 2020). Organizations utilize a combination of people, policies, processes, user education, and technologies to safeguard their assets against cyber-attacks that can compromise systems, steal valuable information, and damage reputation (Jalali et al., 2019; Yeoh et al., 2022). As the frequency and types of cyber-threats increase, organizations' need for cybersecurity also increases with it (Verizon, 2022).

[1] The focus of this study is on organizational digital assets.

Within cybersecurity, IR is an organized approach to detect, contain, and eradicate cyber threats as well as to restore business operations to normal in a timely and cost-effective manner (Ahmad et al., 2021). A cybersecurity incident is an unexpected or unwanted cybersecurity event, or a series of such events, that have a significant probability of compromising business operations (Cichonski et al., 2012; Khan et al., 2021). The lack of an agile approach in detecting and responding to incidents can lead to longer recovery times, increased costs, and further damage to an organization's cybersecurity effectiveness (He et al., 2022). That is why organizations usually establish a Security Operation Center (SOC), which is a centralized function within an organization employing people, processes, and technology to continuously monitor and improve an organization's cybersecurity posture while preventing, detecting, analyzing, and responding to cybersecurity incidents (Kavanagh et al., 2021; Kotsias et al., 2022).

2.2. Big data analytics in cybersecurity IR

Organizations are collecting increasingly large amounts of data as they perform their business operations, for example, data related to supply chain, sales, accounting and finance, operations, and customers (Awan et al., 2021; Ranjan and Foropon, 2021). Today, maintaining large data repositories is part of the organizational business model (Grover et al., 2018). However, the collection of *big data* does not necessarily generate value for organizations (Chen et al., 2012; Müller et al., 2016). What is new, and what makes big data valuable, is when organizations apply analytics to further their strategic objectives (Simsek et al., 2019). According to Mikalef et al., p.2), BDA capability is "*the ability of a firm to effectively deploy technology and talent to capture, store and analyze data, toward the generation of insight*". BDA capability gives organizations a holistic approach to collecting, integrating, and analyzing the 5 V data-related dimensions (velocity, volume, veracity, variety, and value) and thereby creating actionable insights for measuring performance, delivering sustained value, and establishing competitive advantages (Gupta and George, 2016; Jha et al., 2020; Mikalef and Krogstie, 2020). Below, we apply the key characteristics of BDA capability in the context of cybersecurity IR.

First, organizations are now able to capture new sources of data that they were not able to capture before (Müller et al., 2016; Naseer et al., 2017). As a result, the rate of cybersecurity data generation has significantly increased. The variety in sources of cybersecurity data is extremely broad, for example, operations data, social media, network logs, threat intelligence, NetFlow data, firewall logs, security information and event management (SIEM) data, intrusion detection system data, intrusion prevention system data (Naseer et al., 2021b; Eastman and Versace, 2015). Most of this data has always been available, but organizations were not able to capture and integrate this into a single source of truth until novel technologies and methods in BDA were developed and used in cybersecurity.

Second, organizations now have to deal with increasingly large volumes of data due to the growth in data sources (Gupta and George, 2016; Wang and Jones, 2021; Wixom and Goul, 2014). As storage costs have decreased significantly due to the introduction of cloud-based platforms and solutions, all of the aforementioned data that was once retained only for a finite time can now be stored in large data storage systems and data sets indefinitely (L. Da Xu and Duan, 2019; Z. Xu et al., 2016).

Third, the increasing number of data sources and the rate of data generation has resulted in a larger variation in the types of data. Organizations now collect incident-related data that range from highly structured data sets to highly unstructured data sets (Mikalef and Krogstie, 2020; Phillips-Wren et al., 2015). Historically, most data available for cybersecurity analysis was in a structured format (Eastman and Versace, 2015). However, the types of data being captured today range from highly structured and transactional data sets (customer relationship data, financial accounting data) to highly unstructured data

extracted from social media, emails, security logs, threat feeds, and new data sources that are being created through a combination of existing data sources (Verizon, 2022).

The main issue for organizations is not the high volumes of data, the diverse types of data, the collection of data, or the storage of data; but rather how organizations harness this data to generate value in IR. To summarize, organizations are increasingly exploring the role of BDA in enhancing their IR processes and overall enterprise cybersecurity performance (Naseer et al., 2021a). However, what dimensions of BDA-embedded dynamic capabilities are required to enable agility in IR is a paramount strategic question that is yet to be fully understood, providing the research focus for the remainder of the current study.

2.3. Conceptualizing big data analytics-embedded dynamic capabilities in the IR context

Capability is defined as the integration and coordination of strong, repetitive abilities used effectively and appropriately in response to varied, familiar, and unfamiliar circumstances (Nagarajan and Prabhu, 2015). Building on the concept of capability, dynamic capabilities can be classified by three main processes: (a) coordination/integration (a static concept), (b) learning (a dynamic concept), and (c) reconfiguration (a transformational concept) (Teece et al., 1997). Dynamic capabilities theory is an extension of the resource-based view, which theorizes that 'when firms have resources that are valuable, rare, inimitable, and non-substitutable, they can achieve sustainable competitive advantage by implementing fresh value-creating strategies that cannot be easily duplicated by competing firms' (Barney et al., 2001; Schilke and Helfat, 2018). Past research has examined the role of IT in information systems research on Dynamic Capabilities as (a) IT as an enabler of dynamic capabilities, that is, IT artifact encompasses assets or capabilities that enable the emergence of dynamic capabilities and (b) IT as embedded in dynamic capabilities, that is, IT aspects are embedded in the development of dynamic capabilities (Steininger et al., 2022). In this study, we conceptualize BDA-embedded dynamic capabilities as IT-embedded dynamic capabilities and define them as an organization's ability to integrate, mobilize and deploy BDA-based resources to respond to cybersecurity incidents and threats efficiently and effectively.

Though easy to adopt, BDA-embedded dynamic capabilities are difficult to develop in the context of IR as it requires coordination, integration, and reconfiguration of both BDA and cybersecurity resources such as people, processes, technologies, and data to address the dynamic, evolving, and complex cyber threat environment. Organizations cannot simply acquire BDA-embedded dynamic capabilities; they have to build them through the process of converting raw resources into high-end capabilities (Schilke and Helfat, 2018; Steininger et al., 2022).

Past research has used technology as the main resource to study the application of BDA in cybersecurity IR (Sarosh et al., 2021; Terzi et al., 2017; Wang and Jones, 2021). In this study, we argue that technology alone as a resource will not make a sufficient difference unless it is complemented with the right people, processes, and data to transform BDA from a resource into a capability in IR. To develop BDA-embedded dynamic capabilities, organizations need to introduce new processes, train people who can leverage technology, and nurture the culture of data-driven decision-making in their IR practices (Ferdinand, 2015; Lakshmi et al., 2021). Taking this uniqueness into account, an absence of people, processes, and data-related resources will negatively affect the organization when leveraging the true value of technology resources. However, the presence of people, processes, and data resources not only helps the organizations to build a culture of informed decision-making, but also assists when utilizing the technology resources to an extent that cannot be compared to others, making it a valuable, rare, inimitable, and non-substitutable capability for an organization. It is therefore evident that the development of BDA-embedded dynamic capabilities is highly dependent upon the utilization of all analytical resources (de Camargo Fiorini et al., 2018). Therefore, in this study, we explore how integration, coordination, and reconfiguration of analytical resources such as people, processes, technology, and data enable agility in cybersecurity IR through the development of BDA-embedded dynamic capability.

2.4. The need for agility in cybersecurity IR

IR is one of the core areas of a successful cybersecurity program (Kotsias et al., 2022). The IR process is crucial for organizations as they cannot always prevent breaches and a swift response to a cybersecurity incident can reduce the impact on organizational reputation and competitive advantage (Naseer et al., 2023).

To effectively address cybersecurity attacks and data breaches, organizations require quick detection so that they can respond in an agile manner (Grispos et al., 2017, 2014; Siregar and Chang, 2019). The longer a cybersecurity event or incident is left undetected, the more difficult it is for organizations to accurately measure the damage the attack may have caused both to themselves, as well as to their partners and customers (Kavanagh et al., 2021). Our review of the cybersecurity IR literature suggests that organizations mainly invest in building preventive controls that can deal with known cyber threats, rather than in developing a sophisticated and dynamic response capability that can address complex, unknown, and new cyber threats (Baskerville et al., 2014; Naseer et al., 2016a; Shin and Lowry, 2020). Consequently, organizations are better able to deal with cyber threats that are static and predictable. But, they are more vulnerable to unpredictable, dynamic, and new cybersecurity attacks (Ahmad et al., 2021; Naseer et al., 2018; Naseer et al., 2016b). In this paper, we argue that organizations must develop a dynamic IR capability that enables them to proactively monitor cybersecurity events and provide cybersecurity executives with actionable insights in an agile and timely manner to stop the attack before it can cause damage.

Baskerville et al. (2014) in their seminal paper highlighted *agility* as a key feature of the dynamic IR capability. Agility in IR is defined as "the extent to which an organization can add and/or reconfigure its IR resources and processes to detect and respond to unpredictable, unknown, and new cybersecurity threats" (Naseer et al., 2021a, p. 7). While organizations are paying increasing attention to enabling IR agility, not enough is known about how agility can be achieved in IR (Baskerville et al., 2014; Grispos et al., 2014; He et al., 2022; Janicke et al., 2021). Therefore, in this study, we explore the specific dimensions of BDA-embedded dynamic capabilities that enable agility in cybersecurity IR.

3. Research methodology

Given limited evidence about what dimensions of BDA-embedded dynamic capabilities enable agility in cybersecurity IR, we employed a case research method to explore the research question. Both BDA and IR are multi-faceted and complex phenomena that are embedded in an organizational context (Langley, 1999). Therefore, investigating these phenomena through relevant stakeholders' interpretations is more suitable than applying a quantitative approach (Klein and Myers, 1999). We adopted an exploratory approach to be open to unexpected and novel findings and thereby followed the guidelines for inductive research proposed by Gioia et al. (2013). The application of the case research method not only provided us with contextual richness but also allowed us to gain a nuanced understanding of the phenomena (Davison and Martinsons, 2016).

3.1. Case background

Our empirical setting is a multinational financial organization FinSol (a pseudonym). FinSol is recognized as a successful financial company employing more than 15,000 employees. We conducted this study with the IR unit of FinSol. We selected FinSol because it was using state-of-

the-art cybersecurity solutions such as a security information and event management system (SIEM), an Intrusion detection system, an intrusion prevention system, and cyber threat intelligence feeds and databases, which were used to monitor and make sense of cybersecurity events. FinSol also had a dedicated SOC with 25 employees covering roles such as cybersecurity analysts, cybersecurity architects, threat hunters, and the SOC manager. In addition, the cybersecurity IR team at FinSol had a wide repertoire of experiences and in-depth domain knowledge of using BDA for IR.

The chief information security officer (CISO), SOC manager, and cybersecurity analysts used cybersecurity analytics tools, that is, ArcSight and Splunk to collect, analyze, and correlate cybersecurity events data to generate actionable insights. In addition, FinSol also used a performance management system to continuously monitor and assess the organization's current cybersecurity posture and measure the performance of the SOC team to continuously improve their processes and thereby reduce cyber risk. For example, the SOC manager analyzed key performance indicators such as the average time the SOC takes to detect an incident, the number of security incidents detected and processed by the SOC, and the average time that transpires before the SOC takes action and neutralizes the threat to track the scale of activity in the SOC, and how effectively analysts are handling the false positives and workload. Finsol used commercially available, but customized products to source approximately three billion cybersecurity events data in raw form from more than fifty separate data sources each day. The cybersecurity logs and events data were ingested in the Splunk Enterprise for analytics, and the cybersecurity IR team used it to conduct thorough forensic investigations into the origins of a breach or validate emerging threats to gain deeper insight into the performance of their security efforts.

At the time we conducted this study, FinSol was in the process of incorporating big data analytical systems and practices in its IR. This gave us the opportunity for an in-depth exploration of what dimensions of BDA-embedded dynamic capabilities enable agility in IR in a rich organizational context.

3.2. Data collection

Consistent with the exploratory nature of our study, we conducted ten semi-structured interviews with key personnel at FinSol's IR unit to collect qualitative data (Gioia et al., 2013). The success of any qualitative research based on interviews depends on the number of interviews conducted and the quality of the experts interviewed (Schultze and Avital, 2011). While limited, the interviews were sufficient to gain a deep understanding of the phenomena. Although the interviews formed the primary source of data, they were corroborated by secondary data such as organizational documents, internal publications, field notes, and onsite observations. Multiple data collection sources not only enabled triangulation but also offered stronger substantiation of theoretical constructs (Eisenhardt, 1989). The participants of our study actively used BDA to analyze cybersecurity events and represented distinct roles within the cybersecurity IR unit (See Table 1).

Onsite data collection was guided by an interview protocol. Access to FinSol was difficult to achieve since FinSol was quite sensitive to any academic investigation. FinSol's Chief Information Officer was the chief guest speaker at a conference where the lead investigator of this study was presenting their research work. At the conference, the lead investigator discussed the objectives and significance of the research project with FinSol's Chief Information Officer and that opened the door for conducting a case study at FinSol. The full investigation and data collection started after signing a non-disclosure agreement to keep the participant identities anonymous and prevent the leakage of sensitive information. Interviews were recorded and transcribed with participant consent. Each interview was conducted onsite at FinSol's main office and lasted between one and two hours. As the data collection process continued, we continuously revised the interview protocol based on informant responses (Gioia et al., 2013). During the interviews, we asked participants to provide specific examples to gain a deeper understanding of the phenomena under investigation (Schultze and Avital, 2011). As the interview concluded, participants were asked for further reflections on the examples they gave during the interviews.

Table 1
Interviewee profiles.

Level of position	Details of Position (Number of interviews)	Experience (cybersecurity, analytics) years
Top Management	• Chief Information Officer (1)	(20, 30) years
	• Chief Information Security Officer (2)	(28, 25) years
Middle Management	• General Manager, Technology, Information Security & Operations Risk (2)	(30, 25) years
	• Director of Cybersecurity Analytics (2)	(15, 23) years
	• Cyber defense Architect (1)	(22, 16) years
Security Operations center (SOC)	• Head of Threat Intelligence (1)	(15, 10) years
	• SOC Manager (2)	(10, 8) years
	• Threat Hunter (1)	(9, 7) years
	• Senior Cybersecurity Analyst (2)	(8, 6) years
	• Cybersecurity Analyst (1)	(3, 1.5) years
Total number of interviews = 15		

As our data structure took shape after the initial analysis of the qualitative data, we conducted five more follow-up interviews with the Chief Information Security Officer, General Manager of Technology, Information Security & Operations Risk, SOC Manager, Director of Cybersecurity Analytics, and Senior Cybersecurity Analyst. These assisted in gaining deeper insights into the usage of BDA in cybersecurity IR at FinSol over time. Even though the number of interviews is limited, following codification, we assured ourselves that data saturation had been reached after the initial round of interviews, at least for this explorative study (Glaser and Strauss, 2017).

3.3. Data analysis

We analyzed our data following the guidelines provided by Gioia et al. (2013). During our data analysis, we specifically looked for indicators of how BDA was used by the cybersecurity IR unit in their daily operations. It is the everyday practice of BDA in IR that constitutes our unit of analysis. We employed constant comparative techniques and a combination of open, axial, and selective coding to analyze the interview data (Strauss and Corbin, 2014). We used NVivo software to code the transcripts and notes.

In the first stage, open coding was done to develop first-order concepts from interview data using the informants' wording and terms (Gioia et al., 2013). Next, we did axial coding to analyze the first-order concepts by looking for linkages or overlaps among first-order concepts to compile these into higher-order themes. In this stage, we relied on our knowledge and the existing literature to analyze and develop themes that explained the data. We then developed the second-order themes following an iterative process. During these iterative cycles, the first-order concepts were revised, merged, and sometimes abandoned to reach a higher level of abstraction and to arrive at eight second-order themes (Gioia et al., 2013). Lastly, selective coding was employed to combine the eight second-order themes into two aggregate dimensions that captured the overarching concepts relevant to the understanding of what dimensions of BDA enable agility in cybersecurity IR. Fig. 1 presents an example of the data structure capturing the key concepts and themes that emerged from our data analysis.

An example of a data table that supports emergent concepts and themes is also included (see Appendix A). Although we provide only a few examples of raw data, there are numerous examples of first-order

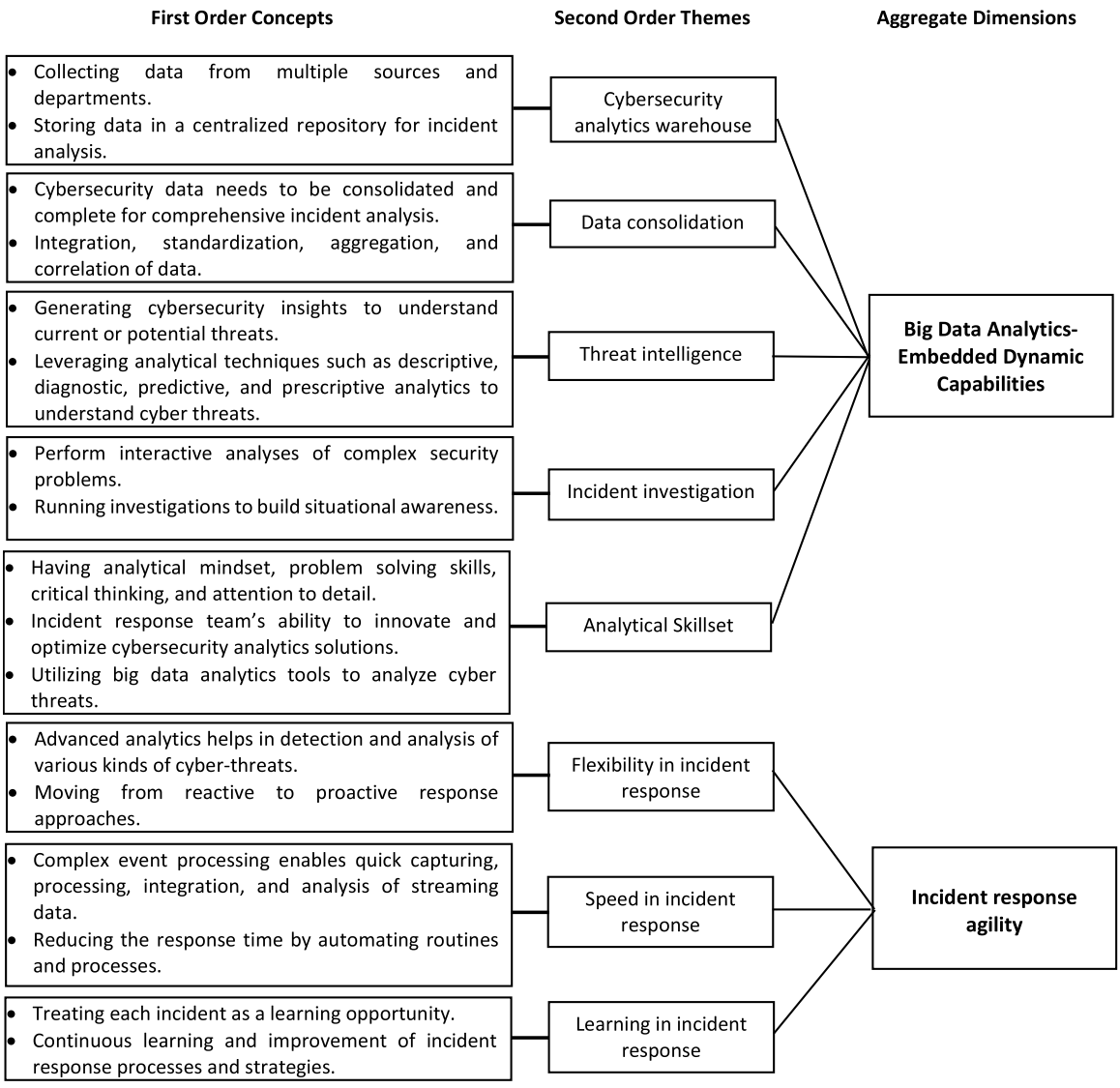

Fig. 1. Data structure example.

concepts and second-order themes. The themes consist of theoretically distinctive concepts that emerged from the data when analyzed at a more abstract level. The data structure shown in Fig. 1 lays the foundation for case analysis that is presented in the next section as follows.

4. Case analysis – an illustrative story

The story illustrates FinSol's IR unit transformation journey in developing BDA-embedded dynamic capabilities and thereby enabling agility in their cybersecurity IR. From 2016, FinSol's IR strategy particularly focused on utilizing BDA for threat detection and response. FinSol's Chief Information Security Officer Stated:

> *We are on that journey right now. Around 12 months ago we reviewed our cybersecurity strategy. One thing that came very clear through the review was, we were very weak in our incident detection and response capability. We had an immature incident management practice. So, we then understood that to be able to improve our detection and response capability we needed to start collecting and analyzing events data from as many sources as possible…Without BDA, we were relying on gut feeling and instincts. So, our response strategy was with a small "s", and our small "s" strategy was potentially more, therefore, a capability built based on assumption. Now our [response] strategy with a capital "S," based on analytics is far more powerful as it is underpinned by tangible fact-based information, which means that our [response] strategy is targeted, it is precise, it is dependable, and it is actionable.*

The transformation journey of incorporating BDA in IR at FinSol was evolutionary. FinSol's Director of Cybersecurity Analytics explained the evolution of BDA at FinSol in four stages: manual analysis, basic analysis, advanced analytics, and pervasive analytics as follows:

> *Historically, the threat analysis and incident investigations were done manually, and the security analytics warehouse was quite a siloed function. Analysis was mostly done on traditional structured data sources. That is historical. In the last two to three years, we have invested heavily in more modern security analytics platforms that can handle unstructured data. So, we specifically have a tool called Splunk where we correlate logs from the servers, applications, and databases to determine what we call indicators of compromise, actionable events, or emerging threats…We have also developed an advanced analytics solution for user and entity behavior analytics that uses AI and machine learning to assess risks and mitigate threats before they cause any damage.*

We explain the key dimensions of BDA-embedded dynamic capabilities (cybersecurity analytics warehouse, data consolidation, threat intelligence, incident investigation, and analytical skillset) in each of

these stages below.

4.1. Manual analysis

At the start of the transformation journey, manual analysis was the go-to method at FinSol for generating insights related to cybersecurity incidents. In manual analysis, there was no centralized repository to integrate and store data such as a cybersecurity analytics warehouse. Data was collected from multiple organizational units and stakeholders, for example, data center administrators, network teams, communication server teams, and applications teams. However, the entire manual data processing was cumbersome, time-consuming, and error-prone. FinSol's General Manager, Technology, Information Security & Operations Risk explained that:

> *Data is the foundation for generating cyber analytics insights. However, the data was manually collected and transferred from one place to another. Given the amount of manual data processing we needed to do and coupling it with the need for attention to detail, errors were likely to occur…therefore, gaining a comprehensive view of the cyber threat environment was difficult and time-consuming with manual analysis.*

The IR team was capturing cybersecurity events and log data only after the incident was discovered. As data capture was reactive rather than proactive, the discovery of the original point and time of compromise was difficult. FinSol's Head of Threat Intelligence noted that:

> *Most of the time we were not able to validate or understand the extent of the cyber threat. This is because the cybersecurity event logs which were not correlated, incomplete, and also not consolidated into a centralized repository. This made validating the time of the initial compromise very difficult.*

Although Incident responders used BDA techniques such as descriptive analytics to generate insights on past or current cybersecurity events, they had limited consolidated data to perform such analytics. Therefore, incident investigations were not complete because the data was not fully integrated or simply not available to paint a holistic picture. FinSol's Director of Cybersecurity Analytics stated:

> *Performing analytics on data drawn from one channel or touchpoint source can be helpful, but what we needed was to integrate and analyze data from multiple sources to generate meaningful insights.*

4.2. Basic analytics

In the next stage of the transformation, FinSol developed a centralized repository to integrate and store cybersecurity data such as a cybersecurity analytics warehouse however, it was still not the main source for data manipulation and analysis. Enterprise-wide standards for cybersecurity data naming and storage management were also introduced. In particular, FinSol used ArcSight (a SIEM solution) as the main centralized repository to standardize, retain, aggregate, correlate, and analyze log data. As FinSol's Cyber defense Architect noted:

> *We've got logs coming into ArcSight and they go through at least one or two levels of transformation…So ArcSight is the central place to collect events and alerts; aggregate and analyze activity from many different resources.*

Incident responders used a combination of both descriptive and predictive analytics to generate behavior-related insights. Some of the analytical tasks such as data collection, integration, and analysis were automated but these were not yet integrated into the mainstream IR processes. FinSol's SOC Manager highlighted the main challenge their IR team faced was around using high-quality logs for behavior analytics as follows:

> *So,* log *quality is a big challenge that I do not think people recognize. Attack techniques just keep advancing, you cannot rely on vendor tools to detect these things. You do need a behavioral analytics capability. But you can say "Oh, we have got a behavioral platform in machine learning so now we should be covered. Behavior analytics is very dependent on the quality of logs that are coming in. Are you getting the right logs coming in? And are those logs the right quality for such analytics?*

Having said that, more data was available to incident responders for incident-specific investigations. Logs from multiple sources were extracted and loaded into the SIEM for data integration, aggregation, and correlation. In addition, metadata and network data were incorporated to enrich the examination, analysis, and reporting of cybersecurity incidents, which helped establish the chain of custody. Consequently, incident investigations became more thorough and complete. FinSol's Senior Cybersecurity Analyst stated:

> *Because the logs were integrated from multiple sources including IDS, IPS, communication servers, and firewalls, and enriched with network data [and metadata], our investigation became more repeatable and complete, and the chain of custody was easy to establish.*

4.3. Advanced analytics

At this stage of transformation, the cybersecurity analytics warehouse became the single source of truth and centralized repository for cybersecurity analytics. Data was sourced and integrated from multiple sources and was available to the incident responders for in-depth incident investigations. In addition, data capture routines were automated at relevant source systems to capture relevant data such as network traffic data, system logs, application logs, security events logs, and Endpoint data as well as every available piece of metadata such as timestamps, user id and account information, and file metadata. Therefore, accurate and timely information related to the risk exposure and cyber threat environment was available to incident responders which, in turn, developed their situation awareness. The Director of Cybersecurity Analytics explained that:

Advanced analytics involved capturing metadata and automation of data capture processes to gain visibility into the most relevant insights related to cyber risk to continuously manage our risk exposure and keep it within the appetite of the organization…this helped us to develop situational awareness which meant that we had timely and accurate information related to potential cyber threats and about our cyber threat environment.

At the advanced analytics stage, the focus was on building the threat hunting capability. For that, FinSol optimized their data retrieval processes using indexes, and therefore cyber events data became highly searchable. To build a comprehensive context, threat intelligence feeds were integrated while doing incident investigations. Advanced analytics was different from basic analytics not only because the data was more readily searchable, but also because all incident-related data was available and enriched with reliable threat intelligence feeds. Threat Hunter at FinSol stated that:

> *We also have a threat hunting capability which is built on reliable threat intelligence feeds to find adversaries hiding in our network. So, at the moment that is where we are building indexes to optimize data retrieval and writing our script to proactively search for threats that are lurking undetected…If the commercial vendor tools are not filling all the gaps, we will fill the gaps with our scripts or use the tools where we can and look for events that we believe would happen if an attack is happening.*

At this stage, FinSol also built a Data Lake environment using open-source technologies to store raw cybersecurity data and interacted with the data using different analytical tools. Cyber defense Architect noted that:

It is a Hadoop-based platform comprising open-source technologies. The reason we made that decision was that we wanted to have an environment where the data lake contains all our data, we can interact with it using any script or any API from a platform-neutral perspective because previously a lot of our data was sitting in ArcSight, and you cannot interact with it or use other tools to process that data.

Finally, using advanced analytics, cybersecurity analysts were able to fully assess, analyze and mitigate the compromise in hours, not days or weeks. Unlike at basic and manual analytics stages, cybersecurity analysts were able to quickly source, integrate, analyze the relevant data using the combination of descriptive, diagnostic, and real-time analytical techniques and thereby developed a comprehensive understanding of the cybersecurity incidents. For example, understanding the attack vectors used in the past incidents and classifying them based on type, frequency, and impact (descriptive analytics), measuring the response time and identifying the underlying causes and factors contributing to the incident through root cause analysis (diagnostic analytics), coupled with monitoring and analysis of streaming data for real-time event correlation and anomaly detection (real-time analytics) enabled FinSol to detect and respond to potential cybersecurity incidents in a proactive manner. FinSol's Chief Information Security Officer explained this as follows:

With advanced cyber analytics, we can fully analyze, evaluate, and mitigate compromises in hours, not days or weeks. This is because we can source, integrate, and analyze the relevant data very quickly and analyze it using different analytical methods [descriptive, diagnostic, and real-time] to determine the actual root cause…in response, we can then implement corrective measures and fine-tune controls. For example, to deal with malware proactively, we look for people accessing websites on the internet that have only recently been registered because historical analysis showed that there is a high probability that these websites may be malicious. When attackers want to attack something, they'll get their malware onto a machine, or they'll do a web drive-by. So, the websites that the malware is communicating back to or the website that gets people infected, they're often only registered very recently because they just start up a website to do an attack. We use real-time proxy logs to continuously monitor all the domains that everyone is visiting. If we're already aware of the domain, we just leave it. But if there is a domain we have never seen and it was created in the last 30 days, we get an alert on the dashboard. The level 2 analyst then analyzes such domains and determines "Is this domain actually malicious?"

4.4. Pervasive analytics

In the final stage of transformation, Finsol focused on embedding analytics into the core of its cybersecurity operations and used it to improve at all stages of its IR process. This involved developing use cases where analytics can make immediate improvements in each phase of the IR process. FinSol's General Manager, Technology, Information Security & Operations Risk stated that:

We developed a number of use cases where analytics could add value to start with and then we expanded from there. For example, analyzing historical incident data to identify potential vulnerabilities and risks. This helped in the preparation by developing IR plans and testing them through simulations…Continuous monitoring and analysis of events data using advanced analytics techniques helped in the detection by identifying patterns and anomalies that indicate a potential threat…Real-time analytics to generate alerts and recommendations to IR teams helped in determining the scope and impact of an incident and also in prioritizing and coordinating the response…using advanced analytics for post-incident analysis helped in assessing the effectiveness of the response and identifying the root cause and opportunities for improvement.

At the pervasive analytics stage, FinSol focused on reducing the number of false positives by leveraging advanced analytics. FinSol's Cyber defense Architect noted that:

When advanced analytics starts to fill the gap, then you can focus on the real attacks. You could potentially reduce the number of staff that you've got that are looking at these very basic alerts because almost, you know, I'd say 80 percent of them are going to be false positive and not worth actioning but you don't know that until you've looked at it. So, one example is malicious code. If there is an alert for malicious code running on a workstation or a server that's been detected, level 1 will go and run certain tools on that workstation to do a collection of valuable information that will be used for the analytics. If it is not a false positive, it goes to level 2, and they do the analysis of that information. In most cases, they can do something like just a commodity malware running on a workstation, just rebuild the server if it hasn't spread more widely. But if the insights show there's a back door on a server and it potentially had people interacting with it, then it will come to the senior team and we'll actually have to try and figure out, Okay. Did they move laterally from this machine? Did it affect the business operations? Did they exfiltrate valuable data? We'll try and answer these questions using advanced analytics. So, it helps to focus on serious, actual threats and not bogged down in false positives.

Pervasive analytics was underpinned by various advanced analytics techniques such as AI, machine learning, and data visualization. The goal for making analytics pervasive was to learn from cybersecurity events/incidents and continuously improve IR strategies, processes, and procedures. FinSol's Director of Cybersecurity Analytics explained this as follows:

We have an advanced analytics engine for big data, AI, and machine learning such as Spark and we hired a data scientist to help us with that… So, one example was to try and detect lateral movement from NetFlow, so looking at every single connection between every single pair of hosts in the network and then if there is a particular flow of data that has not been seen before, whether that be IP address communicating to IP address that has never happened before or a report that those two have never communicated ever before, those should generate an alert. So, it is useful in learning adversary behavior.

4.5. Moving towards agile cybersecurity IR: a conceptual framework

Fig. 2 shows the framework that we have developed based on the analysis of our data. The framework proposes four distinct stages of analytics usage in the IR process i.e., manual analysis, basic analytics, advanced analytics, and pervasive analytics. The key dimensions of BDA-embedded dynamic capabilities in IR include cybersecurity analytics warehouse, data consolidation, threat intelligence, incident investigation, and analytical skillset. The agile characteristics that the utilization of BDA-embedded dynamic capabilities infused into the IR are flexibility, speed, and learning. Table 2 presents key features of BDA-embedded dynamic capabilities in cybersecurity IR at the manual, basic, advanced, and pervasive analytics stages.

Agile IR requires management, integration, and analysis of high-volume and high-velocity data from various data sources to quickly discover anomalies and/or attack patterns. For that, FinSol not only developed advanced analytics beyond simple rule-based approaches but also the ability to run analysis on a large amount of current and historical data. FinSol's Chief Information Security Officer explained that:

Rules are defined *in the SIEM and mostly those rules will generate an alert. So, a lot of it is pretty much signature-based detections and it's centered around the controls we have…but we also run analytics on current and historical data using our own custom* script *where necessary. If the commercial vendor tools aren't filling all the gaps, we'll fill the gaps with our own scripts or use the tools where we can to look for things that we believe would happen if an attack is happening.*

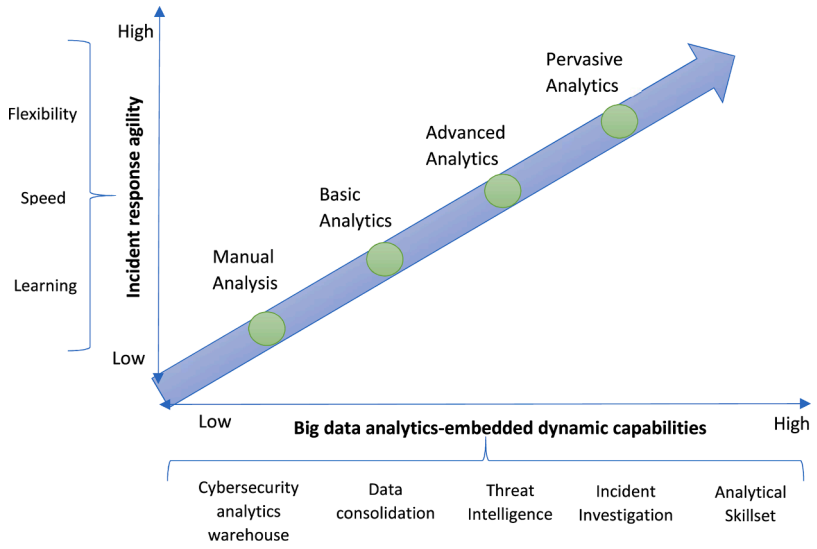

Fig. 2. Enabling IR agility through big data analytics-embedded dynamic capability.

Table 2
Big data analytics-driven cybersecurity IR.

Dimension	Manual analysis	Basic analytics	Advanced analytics	Pervasive Analytics
Cybersecurity analytics warehouse	• No centralized data repository • Data needs to be collected from multiple sources and departments; there is no standard format or storage structure	• A centralized data repository exists but is still not the main source for BDA • There are enterprise-wide and defined standards for naming and storing cybersecurity data, but data is not always easily available	• The cybersecurity analytics warehouse is the single source of truth for BDA • There are no data silos and data are easily available for in-depth analysis	• Analytics is available at the point of the decision and embedded in every stage of the IR process, making analytics both proactive and pervasive. • Incident investigations are underpinned by various advanced analytics techniques such as AI, machine learning, and data visualization. • The focus of the IR team is on learning from cybersecurity events/ incidents and continuously improving the IR strategies, processes, and procedures.
Data consolidation	• Limited integration of the data • An analytics architecture exists but analytical systems work in silos	• SIEM is usually in place to integrate, standardize and correlate data	• Cybersecurity data is integrated and complete • Incident-related data is enriched with reliable threat intelligence feeds • There are clear mechanisms in place to connect new data sets with existing data.	
Threat intelligence • Using descriptive and diagnostic analytics to generate cybersecurity insights • Analytics is done only to achieve specific targets and results	• Using descriptive, diagnostic, or even predictive analytics to generate cybersecurity insights • Some of the analytical tasks are automated but not integrated into the security processes	• The mindset of the IR team is to continuously generate insights using BDA, which makes use of all kinds of data including streaming data. • Using descriptive, diagnostic, predictive, and prescriptive analytics to understand cybersecurity events. • Automation is used to investigate cybersecurity threats		
Incident investigation • Information is not easily discoverable and difficult to validate	• The initial point of compromise is usually determined • Investigations are not comprehensive enough to build situational awareness	• The IR team can generate effective visualizations and new intelligence or insights about cyber threats to provide decision support • Investigations build comprehensive situation awareness		
Analytical skillset • The IR team can use BDA tools but lack critical thinking and problem-solving skills	• The IR team has the specific analytical skillset required to generate incident-specific insights	• Incident responders have critical thinking skills to analyze problems, evaluate alternatives, and optimize cybersecurity analytics solutions.		

This is where BDA-embedded dynamic capabilities infused agile characteristics of speed, flexibility, and learning in IR. First, through the utilization of different analytical methods including descriptive, diagnostic, predictive, and prescriptive at the advanced analytics stage, FinSol enabled flexibility in their IR by generating meaningful and diverse insights about their cyber threat environment. FinSol's Head of Threat Intelligence noted that:

These insights help us in making more objective or in other words scientific decisions. So, descriptive, diagnostic, predictive, and prescriptive analytical methods are vital in understanding what has happened in the cyber threat environment, why it happened, what is likely to happen next, and what can we do about it.

FinSol's Cyber defense Architect provided the following example to explain how threat intelligence and advanced analytics capabilities helped in the detection and analysis of diverse cyber threats in a proactive manner and thereby enabled flexibility in IR:

Threat actors with sophisticated social engineering capabilities consistently target our employees and C-level executives by sending malicious emails through phishing and spear phishing, aiming to steal sensitive information such as their login credentials, customer data or infect the systems with malware. We have threat intelligence feeds in which we use advanced analytics to analyze what is happening and we also participate in threat intelligence sharing communities. On a daily basis, we get feeds from our peers across the industry around phishing campaigns and new emerging malware… Analyzing the indicators of compromise from previous phishing incidents helps in discovering the similarities in the phishing email templates, such as specific wording, visual elements, or infrastructure used for hosting phishing landing pages, including specific domain names or IP addresses… So, while we are investigating a cyber threat or incident, having access to analytical insights [on attack vector, target selection, threat intelligence, and Indicators of Compromise] can be very helpful in understanding the attacker's motives, capabilities, and likely actions.

Second, most of the cybersecurity events data generated by diverse sources came in the form of logs. The main challenge for the IR team at FinSol was to build analytical systems that could integrate the continuously growing stream of data quickly and give correct meaning and context to cybersecurity events in the constantly evolving cyber threat landscape. At the advanced analytics stage, FinSol built a combination of analytical systems such as complex event processing, data lake, and SIEM to capture, process, and integrate streaming data and thereby analyzed cause-and-effect relationships among cybersecurity events swiftly. According to FinSol's Director of Cybersecurity Analytics:

Using complex event processing systems, we continuously monitor cybersecurity events because here, the events act as a trigger. The goal is to integrate and analyze streaming data on the fly and take appropriate actions based on the alerts against suspicious events.

Although SIEM solutions play an integral role in integrating, standardizing and correlating data, FinSol's SOC Manager highlighted the economic challenges associated with SIEM solutions as follows:

We discussed the cost of licensing of SIEM solution. Economically we cannot store information for extended lengths of time. So, we may find that we can only store detailed events data for up to six months. We cannot afford to store Petabytes of information on incident and event data that consists of two to three or even five year period. So again, economically we have to constrain ourselves to the amount of data that we can actually collect and analyze.

FinSol's Chief Information Security Officer further elaborated the implications of cybersecurity data retention on dealing with cyber events as follows:

SPLUNK has a reputation of being very expensive and reason why it is expensive is because of the charges on data ingestion model. So, it's not just the case of throwing everything at the ingestion. You have to actually choose the data you send for analytics. So, there is a chance that you miss events in trying to save money and in doing so you are throwing away the data you actually needed…In terms of how you would address this challenge, the key is to strike a balance that aligns with our risk tolerance and security objectives, considering the specific nature threats and the need for timely and accurate incident response.

FinSols General Manager, Technology, Information Security & Operations Risk noted that measuring the risk of data retention is a complex process that requires the combination of legal, organizational and technical risk assessments.

Actually it's a complex process that involves first of all assessing if we are compliant with the legal requirements [legal]…evaluating the criticality of the data being retained [organizational] and assessing if the security controls in place are good enough to deal with the potential vulnerabilities and threats to the stored data [Technical].

Third, the use of visual and advanced analytics techniques at the pervasive analytics stage enabled FinSol's IR team to develop proactive response strategies and provided decision support to cybersecurity managers. Finsol's SOC Manager stated that:

Visual analytics aids our decision support. For example, visualizing network data to identify a spike in traffic to a specific IP address or a sudden increase in failed login attempts…proactive response in these cases was to block traffic from the suspicious IP address and activate more layers of multi-factor authentication to prevent further unauthorised login attempts.

By embedding analytics in each stage of the IR process, the IR team at FinSol developed the awareness, skillsets, and vision to continuously learn and improve their IR resources and capabilities. FinSol's Chief Information Officer noted that:

Analytics definitely improves the IR processes; however, it is something that came at a very high maturity level. We defined meaningful metrics to monitor and assess the performance of response processes and the SOC team… the goal was to continuously learn and improve our detection and response capabilities.

FinSol did not simply move from the manual analysis stage directly to the pervasive analytics stage. It was a transformational journey where each milestone on the way added value to the IR process. Getting to the pervasive analytics stage and enabling agility in IR required a combination of the right people, tools, processes, data, training, and overarching analytical architecture. FinSol's Chief Information Security Officer explained the milestones for accomplishing this journey as follows:

"First milestone was getting the strategy approved from top management to do something. The next milestone was hiring and forming a new IR team. So, hiring a head of cyber defense and threat intelligence…The next milestone for us was partnering with a specialist provider to set up our security operation center. We now call it the Cyber defense center. The final piece of the puzzle was designing the target analytical architecture that could capture events data from diverse sources in greater volume than at present, consolidate the data into a centralized repository, and finally provide actionable insights which can quickly lead us to the most pressing issues."

5. Discussion

In this study, we examined what dimension of BDA-embedded dynamic capabilities enables agility in cybersecurity IR. Our findings present two key components that drive overall cost and inhibit agility in cybersecurity IR: (1) once the attacker gains access to the organizational network, the length of time it takes to detect the intrusion (Naseer et al., 2023); and (2) once the intrusion or incident has been detected, the speed at it which a response and remediation can be executed (He et al., 2022). BDA-embedded dynamic capabilities help in addressing both components by reducing the time taken to detect and respond to cybersecurity incidents, which ultimately leads to cost savings and agility in IR. We discuss the theoretical contributions and practical implications of our research results in the following subsections.

5.1. Theoretical contributions and propositions

This research presents several important contributions to theory and research propositions emerging from theoretical contributions as identified from the results of this study. BDA can have a transformative effect on organizational business processes (Loebbecke and Picot, 2015; Ranjan and Foropon, 2021). Our results consolidate these observations and highlight the transformative effect of BDA-embedded dynamic capabilities in the cybersecurity IR process. For example, we identify the key dimensions of BDA-embedded dynamic capabilities that enable agility in IR and thereby transform the IR processes, routines, and practices. This supports the study by Chatfield & Reddick (2018) that explained how customer agility is influenced by BDA-enabled business process change and by Tseng et al. (2022) that big data analytics is crucial in enabling agility. In addition, our results reinforce the findings of Jha et al. (2020) that a multitude of factors affects the capability of a company to implement and use BDA. In summary, our framework develops the current conceptualization of BDA-embedded dynamic capabilities and extends the existing literature by identifying its specific dimensions that enable agility in the IR process. Accordingly, the following proposition augments the discussion for subsequent research investigation.

Proposition. *Data consolidation, threat intelligence, incident investigation, analytical skillset, and cybersecurity analytics warehouse are key dimensions of BDA-embedded dynamic capabilities that organizations leverage to enable agility in their IR.*

Similarly, the current conceptualization of analytical capabilities in IR does not specifically deal with big data (Naseer et al., 2023), nor does it explore the role of dynamic capabilities in enabling agility in IR (Baskerville et al., 2014; Grispos et al., 2017; He et al., 2022). Here, we investigated how BDA-embedded dynamic capabilities enable agility in IR over time. We found that enabling IR agility using BDA-embedded dynamic capabilities is a transformational journey in which the IR team moves from manual to basic, then to advanced, and ultimately to pervasive analytics. As the IR team advances through these stages, they continuously integrate, coordinate, and reconfigure their analytical and cybersecurity resources. At the pervasive analytics stage, IR teams can detect and respond to unknown, complex, and unpredictable cybersecurity threats in an agile and proactive manner. Thus, in integrating insights from previous research that highlights the transformational role of digital technologies in redefining organizational value proposition (Wessel et al., 2021) and enabling agility (Elia et al., 2022; Salmela et al., 2022), the current study indicates how these insights can be extended. That is, BDA-embedded dynamic capabilities play a transformational role in enabling IR agility over time by integrating, building, and reconfiguring IR resources, routines, and processes. These findings, therefore, offer further empirical evidence thus extending the dynamic capabilities theory and use of BDA in IR.

Proposition. *BDA-embedded dynamic capabilities enable agility in IR when an organization transforms from manual analysis to basic analytics, then to advanced analytics, and ultimately to pervasive analytics in IR.*

Existing research has explored the role of BDA in the context of IT as an enabler of dynamic capabilities (Steininger et al., 2022). For example, Mikalef et al. (2021) examine the role of BDA in the development of dynamic capabilities and identify inertial forces that emerge during different phases of diffusion. Gupta & George (2016) argue that organizations that develop a BDA capability can better respond to market changes and thereby have a stronger sensing capability. Similarly, Côrte-Real et al. (2020) noted that BDA capabilities can create significant value in business processes if supported by a good level of data quality which, in turn, leads to a better competitive advantage. Adopting a more holistic perspective, Conboy et al. (2020) explain how BDA can be leveraged to enhance sensing, seizing, and transforming processes. Our findings extend the prior research by conceptualizing BDA-embedded dynamic capability as a specialized IT-embedded dynamic capability (Steininger et al., 2022). Our conceptualization can help improve the understanding of the emergence of IT-embedded dynamic capabilities in the context of IR as they are dynamically formed and evolved. Through the framework, we explain how BDA-embedded dynamic capabilities usage at the pervasive analytics stage enhances the IR team's ability to continuously learn from cybersecurity events/incidents and improve IR strategies, processes, and procedures. Thus, the following proposition lays the foundation for subsequent research investigation.

Proposition. *Increasing BDA-embedded dynamic capabilities usage at the pervasive analytics stage enhances the IR team's ability to learn from cybersecurity events/incidents and continuously reconfigure, redesign, and improve their IR strategies, workflows, processes, and procedures.*

Lastly, we posit this is the first study to our knowledge that explores the use of BDA-embedded dynamic capabilities to enable agility in IR. Firms with strong dynamic capabilities can improve their organizational agility so that they are better equipped to detect threats, opportunities, and changes in the environment which, in turn, enables organizations to exploit opportunities for innovation and competitive action (Park et al., 2017; Tallon et al., 2019; Teece et al., 2016). In addition, agility is the key mechanism through which organizations can excel and outperform their competition by responding more proactively to changing business environments (Conboy et al., 2020; Huang et al., 2014). Our study supports these findings and suggests that utilization of BDA-embedded dynamic capabilities infuse agile characteristics of flexibility, speed, and learning in IR. Subsequently, this enables organizations to respond quickly to emerging and dynamic cyber threats. To sum up, given the growing need to address complex and dynamic cyber threats, the extent to which an organization can swiftly modify or alter its IR processes and resources seems to be heavily reliant on its ability to implement and leverage BDA-embedded dynamic capabilities.

Proposition. *Utilization of BDA-embedded dynamic capabilities infuse agile characteristics of speed, flexibility, and learning in IR and thereby enable organizations to detect and respond to cybersecurity incidents in an agile manner.*

5.2. Implications for practice

The findings from the FinSol case study offer several practical insights about using BDA-embedded dynamic capabilities to enable agility in cybersecurity IR. We utilize the Pan & Pee (2020) 3 U framework to demonstrate the practical impacts. The 3 U framework identifies three forms of impactful research outputs, that is, usable, in-use, and useful research outputs to demonstrate practice impact. It also provides checklist questions that help researchers design their studies (Pan and Pee, 2020). The research output from this study will benefit IR teams, cybersecurity managers, and vendors that intend to enable agility in cybersecurity IR using BDA.

5.3. Rethink IR agility

Our framework illustrates that enabling agility in IR using BDA is a journey and an evolutionary process that requires organizations to move from manual to basic, then to advanced, and ultimately to pervasive analytics. This is much like 'we need to learn to crawl and walk before we can run'. As organizations progress through these stages, they need to continuously integrate, build, and reconfigure their analytical resources such as people, processes, technology, and data. This observation expands our existing knowledge of IR agility and reminds practitioners to pay attention to the essential role of dynamic capabilities in enabling IR agility. The use of BDA-embedded dynamic capabilities enables organizations to strengthen their IR process in such a way that infuses speed, flexibility, and learning in their IR. These agile characteristics are critical in the effective mitigation of complex and

dynamic cyber threats.

5.4. Rethink the value of BDA

Our research indicates that even though many BDA tools and practices have been developed in the past few years, their usage in the cybersecurity IR warrants new strategies considering many aspects like zero-day attack detection, unified data architecture, cybersecurity events correlation, data sharing across threat detection systems, real-time analysis of data, automated response, and predictive analytics for anomaly detection. To enable agility in IR, vendors who develop BDA solutions need to understand the transformational role that their BDA solutions may provide to organizations. Building BDA solutions that can quickly automate investigations and forensic analysis, apply complex algorithms, integrate threat intelligence data, provide analytical insights to discover potential cyber threats, and create visualizations that can help IR teams quickly identify patterns and understand the progression of an incident will help their clients enable agility in IR.

5.5. Enable agility in IR

The Director of Cybersecurity Analytics at FinSol noted that: analytical tools and technologies help but what makes incident investigations agile and more complete is having analytical understanding and skills. Our findings consolidate this insight. Cybersecurity executives need professionals in their IR teams that have strong business acumen and communications and analytical skills so that incident responders can understand their business and analyze cyber threats in a broader context efficiently and effectively. Our study suggests that cybersecurity executives need to hire and/or train analytics or cybersecurity professionals with the knowledge and skills required to develop cybersecurity analytics applications and acquire as well as integrate BDA solutions provided by external vendors. For that, cybersecurity executives can: (1) recruit professionals that come from a BDA background and teach them cybersecurity knowledge and processes; (2) teach and upskill their existing cybersecurity professionals that have a traditional cybersecurity background about how to understand and leverage the more advanced analytics capabilities; and/or (3) procure managed security service providers or vendors if they cannot train or hire existing employees while they build up their BDA-embedded dynamic capabilities in IR. Our findings suggest that educating BDA professionals with cybersecurity knowledge is the most suitable option as they can leverage the insights gained from the cybersecurity threat environment and feed them back to the rest of the business to safeguard organizational performance.

> "To me, it makes more sense to get data analytics people and educate them on security as opposed to educating security people to do data analytics. I think that would be the better outcome because they would also then be able to use some of that information that they could garner from the security landscape and then feed that back to the rest of the business to create value." (Chief Information Security Officer, FinSol)

6. Limitations and directions for future research

We offered four propositions in Section 5.1 that were derived from the theoretical contributions of this study and proposed as important future research considerations. The current study also has several limitations that need to be considered. First, the context of our study raises questions about the generalizability of the proposed framework, hence requiring future work to improve it. While our study explains the role of BDA-embedded dynamic capabilities and pervasive analytics in enabling agility in IR, it does not go further to examine how BDA-embedded dynamic capabilities, pervasive analytics, and IR agility impact cyber resilience (an emerging area of cybersecurity research (Goel et al., 2023)). Future studies exploring the link between pervasive analytics, dynamic capabilities, IR agility, and cyber resilience would be useful in this context.

The second limitation pertains to the single case study method. From our study, we cannot conclude that the case organization is in any way representative of how BDA is used in IR in other organizational settings. We make a modest and more limited claim. The explanation of how BDA-embedded dynamic capabilities infuse agile characteristics of flexibility, speed, and learning in IR, in this study, is a step ahead in understanding how BDA may enable agility in IR. Further studies, utilizing the framework that we developed from FinSol's case, would help to assess its generalizability. Therefore, our findings should be interpreted with caution as they are derived from a single case study.

Finally, we invite the researchers to conduct future studies that would extend, reject, or support our findings in other organizational settings. Future studies in other organizational settings can add more depth to the proposed framework by providing rich insights on (1) the knowledge and skills required by the cybersecurity teams to utilize BDA in IR, (2) factors that enable or hinder the development of agile features in IR using BDA, and (3) conditions which affect the utility of BDA in cybersecurity IR. Despite these limitations, our utilization of the practice lens on BDA opens a new direction for BDA research in cybersecurity IR that considers the implications of using BDA-embedded dynamic capabilities to enable agility in IR with actual practice in mind, and our findings lay the foundation for future research that can be undertaken to extend, challenge and confirm our conclusions.

7. Conclusion

Reflecting on the growing adoption of data and analytics in cybersecurity, this research explored the role of BDA-embedded dynamic capabilities in enabling agility in cybersecurity IR. There has been little work on the use of BDA and dynamic capabilities in IR, and there is a significant gap in the literature to address the research question, "*What dimensions of big data analytics-embedded dynamic capabilities enable agility in cybersecurity IR?*" Integrating insights gleaned from the empirical data with existing literature on cybersecurity IR, BDA, and dynamic capabilities theory, we propose a framework that identifies five key dimensions of BDA-embedded dynamic capabilities in IR at four specific stages, that is, manual analysis, basic analytics, advanced analytics, and pervasive analytics. The details of the framework explain how utilization of BDA-embedded dynamic capabilities at the pervasive analytics stage infuse agile characteristics of *speed, flexibility, and learning* in IR. Thus, this research presents a useful insight into using BDA-embedded dynamic capabilities for enabling agility in IR, a link poorly understood to date.

CRediT authorship contribution statement

Ayesha Naseer: Methodology, Data curation, Project administration, Writing – review & editing. **Humza Naseer:** Conceptualization, Methodology, Investigation, Formal analysis, Writing – original draft, Writing – review & editing. **Atif Ahmad:** Writing – review & editing. **Sean B Maynard:** Writing – review & editing. **Adil Masood Siddiqui:** Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Appendix A. - Example of Data Supporting Interpretations of Second-Order Themes

Aggregate Dimensions	Second order Themes	Representative Quotes
Big Data Analytics-Embedded Dynamic Capability	Cybersecurity analytics warehouse	*"Data for security analytics are the combination of internal and external data which is in different formats and different systems."* (Cybersecurity Analyst)
	Data consolidation	*"We needed to integrate data from a variety of sources and the aim was to extract anomalies that may suggest an active threat within the network."* (Cyber defense Architect)
	Threat intelligence	*"The goal of using big data analytics in cybersecurity is to generate cyber threat intelligence and execute complex analysis quickly, ideally close to real-time…to identify changing user patterns, and to perform complex correlations and aggregations across a variety of data sources ranging from application and server logs to user activities and network events."* (General Manager, Technology, Information Security & Operations Risk)
	Incident investigation	*"Unless we have the ability to model anomalous and normal behavior of network assets and people, we will not be able to detect the novel types of cyber-attacks."* (Cyber defense Architect)
	Analytical Skillset	*"Identifying our current level of capability maturity helps us to identify what our gaps are. We can then formulate our strategy to fill these gaps and improve our capability for cybersecurity services over time. We translate that into an actionable roadmap of investment in technology, processes, people, and skills development to try and achieve that outcome to continuously improve our detection, protection, response, and recovery capabilities to protect our information systems and assets."* (Chief Information Security Officer)
IR Agility	Flexibility in IR	*"We use a combination of descriptive, predictive, and prescriptive analytical methods to become more effective and proactive in our cybersecurity IR process."* (Threat Hunter)
	Speed in IR	*"We have developed a Big data analytical system that ingests the streaming data in real-time and analyzes it, correlates values, and blends different cybersecurity events streams together."* (Director of Cybersecurity Analytics)
	Learning in IR	"Advanced analytics helps in reducing the IR time by automating the IR processes…and also learn from past incidents to improve the future detection and response." (Chief Information Officer)

References

Adesemowo, A.K., 2021. Towards a conceptual definition for IT assets through interrogating their nature and epistemic uncertainty. Comput. Secur. 105, 102131.

Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T., Baskerville, R.L., 2021. How can organizations develop situation awareness for incident response : a case study of management practice. Comput. Secur. 101, 102–122.

Awan, U., Shamim, S., Khan, Z., Zia, N.U., Shariq, S.M., Khan, M.N., 2021. Big data analytics capability and decision-making: the role of data-driven insight on circular economy performance. Technol. Forecast. Soc. Change 168 (March), 120766.

Barney, J.B., Wright, M., Ketchen, J.D., 2001. The resource-based view of the firm: ten years after 1991. J. Manage. 27 (6), 625–641.

Baskerville, R., Spagnoletti, P., Kim, J., 2014. Incident-centered information security: managing a strategic balance between prevention and response. Info. Manage. 51 (1), 138–151.

Chatfield, A.T., Reddick, C.G., 2018. Customer agility and responsiveness through big data analytics for public value creation: a case study of Houston 311 on-demand services. Gov. Inf. Q. 35, 336–347.

Chen, H., Chiang, R.H., Storey, V.C., 2012. Business intelligence and analytics: from big data to big impact. MIS Quarterly 36 (4), 1165–1188.

Cichonski, P., Millar, T., Grance, T., Scarfone, K., 2012. Computer Security Incident Handling guide: Recommendations of the National Institute of Standards and Technology. NIST Special Publication, pp. 800–861. Revision 2.800–61.

Conboy, K., Mikalef, P., Dennehy, D., Krogstie, J., 2020. Using business analytics to enhance dynamic capabilities in operations research: a case analysis and research agenda. Eur. J. Oper. Res. 281 (3), 656–672.

Côrte-Real, N., Ruivo, Pedro, Tiago, O., 2020. Leveraging internet of things and big data analytics initiatives in European and American firms: is data quality a way to extract business value? Info. Manage. 57 (1), 1–16.

Creasy, J., Glover, I., 2013. Cyber security incident response guide. CREST. In: https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Procurement-Guide-1.pdf.

Davison, R.M., Martinsons, M.G., 2016. Context is king! Considering particularism in research design and reporting dp. J. Info. Technol. 31 (3), 241–249.

de Camargo Fiorini, P., Roman Pais Seles, B.M., Chiappetta Jabbour, C.J., Barberio Mariano, E., de Sousa Jabbour, A.B.L, 2018. Management theory and big data literature: from a review to a research agenda. Int. J. Inf. Manage. 43 (May), 112–129.

Eastman, R., & Versace, M. (2015). Big data and predictive analytics: on the cybersecurity front line. IDC White Paper, February.

Eisenhardt, K.M., 1989. Building theories from case study research. Acad. Manage. Rev. 14 (4), 532–550.

Elia, G., Raguseo, E., Solazzo, G., Pigni, F., 2022. Strategic business value from big data analytics: an empirical analysis of the mediating effects of value creation mechanisms. Info. Manage. 59 (8), 103701.

Ferdinand, J., 2015. Building organisational cyber resilience: a strategic knowledge-based view of cyber security management. J. Bus. Contin. Emer. Plan 9 (2), 185–195.

Gioia, D.A., Corley, K.G., Hamilton, A.L., 2013. Seeking qualitative rigor in inductive research: notes on the Gioia methodology. Organ Res. Methods 16 (1), 15–31.

Glaser, B., Strauss, A.L., 2017. Discovery of Grounded theory: Strategies for Qualitative Research. Routledge.

Goel, L., Russell, D., Williamson, S., & Zhang, J.Z. (2023). Information systems security resilience as a dynamic capability. Journal of Enterprise Information Management, Advance online publication. doi:10.1108/JEIM-07-2022-0228.

Grispos, G., Bradley, W., Storer, T., 2017. Enhancing security incident response follow-up efforts with lightweight agile retrospectives. Digital Investigation 22, 62–73.

Grispos, G., Glisson, W.B., Storer, T., 2014. Rethinking security incident response: the integration of agile principles. In: Proceedings of the 20th Americas Conference on Information Systems, pp. 1–9.

Grover, V., Chiang, R.L., Ting-Peng, L., Dongosng, Z., 2018. Creating strategic business value from big data analytics. J. Manage. Info. Syst. 35 (2), 388–423.

Gupta, M., George, J.F., 2016. Toward the development of a big data analytics capability. Info. Manage. 53 (8), 1049–1064.

He, Y., Zamani, E.D., Lloyd, S., Luo, C., 2022. Agile incident response (AIR): improving the incident response process in healthcare. Int. J. Inf. Manage. 62, 1–15.

Huang, P.Y., Pan, S.L., Ouyang, T.H., 2014. Developing information processing capability for operational agility: implications from a Chinese manufacturer. Eur. J. Info. Syst. 23 (4), 462–480.

Jalali, M.S., Siegel, M., Madnick, S., 2019. Decision-making and biases in cybersecurity capability development: evidence from a simulation game experiment. J. Strat. Info. Syst. 28 (1), 66–82.

Janicke, H., Smith, R., Maglaras, L., Cook, A., He, Y., Ferra, F., 2021. Agile incident response in industrial control environments. Cybersecurity Issues in Emerging Technologies. CRC press.

Jha, A.K., Agi, M.A.N., Ngai, E.W.T., 2020. A note on big data analytics capability development in supply chain. Decis. Support Syst. 138 (113382).

Kavanagh, K., Bussa, T., Collins, J., 2021. Magic Quadrant for Security Information and Event Management. Gartner Res. 1–41. June.

Khan, F., Kim, J.H., Mathiassen, L., Moore, R., 2021. Data breach management: an integrated risk model. Info. Manage. 58 (1), 1–12.

Klein, H.K., Myers, M.D., 1999. A set of principles for conducting and evaluating interpretive field studies in information systems. MIS Quarterly 23 (1), 67–94.

Kotsias, J., Ahmad, A., Scheepers, R., 2022. Adopting and integrating cyber-threat intelligence in a commercial organization. Eur. J. Info. Syst. 1–17.

Lakshmi, R., Naseer, H., Maynard, S., Ahmad, A., 2021. Sensemaking in cybersecurity incident response: The interplay of organizations, technology and individuals. Twenty-Ninth European Conference on Information System. 1-12.

Langley, A., 1999. Strategies for theorizing from process data. Acad. Manage. Rev. 24 (4), 691–710.

Loebbecke, C., Picot, A., 2015. Reflections on societal and business model transformation arising from digitization and big data analytics: a research agenda. J. Strat. Info. Syst. 24 (3), 149–157.

McMillan, R., & Proctor, P. (2018). Cybersecurity and digital risk management: cIOs must engage and prepare. Gartner Res., January.

Mikalef, P., Krogstie, J., 2020. Examining the interplay between big data analytics and contextual factors in driving process innovation capabilities. Eur. J. Info. Syst. 29 (3), 260–287.

Mikalef, P., Krogstie, J., Pappas, I.O., Pavlou, P., 2020. Exploring the relationship between big data analytics capability and competitive performance: the mediating roles of dynamic and operational capabilities. Info. Manage. 57 (2), 103169.

Mikalef, P., van de Wetering, R., Krogstie, J., 2021. Building dynamic capabilities by leveraging big data analytics: the role of organizational inertia. Info. Manage. 58 (6), 103412.

Müller, O., Junglas, I., Brocke, J., 2016. Utilizing big data analytics for information systems research: challenges, promises and guidelines. Eur. J. Info. Syst. 25 (1), 289–302.
Nagarajan, R., Prabhu, R., 2015. Competence and capability - a new look. Int. J. Manage. 6 (6), 7–11.
Naseer, A., Naseer, H., Ahmad, A., Maynard, S.B., Masood, A., 2021a. Real-time analytics, incident response process agility and enterprise cybersecurity performance: a contingent resource-based analysis. Int. J. Inf. Manage. 59, 1–10.
Naseer, H., Desouza, K., Maynard, S.B., Ahmad, A., 2023. Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics. Eur. J. Info. Syst. 1–21.. https://doi.org/10.1080/0960085X.2023.2257168.
Naseer, H., Maynard, S., Ahmad, A., 2016a. Business analytics in information security risk management : the contingent effect on security performance. In: Proceedings of the 24th European Conference on Information Systems, pp. 1–12.
Naseer, H., Maynard, S.B., Ahmad, A., Shanks, G., 2018. Cybersecurity risk management using analytics: a dynamic capabilities approach. In: Proceedings of the Thirty Ninth International Conference on Information Systems, pp. 1–9.
Naseer, H., Maynard, S.B., Desouza, K.C., 2021b. Demystifying analytical information processing capability: the case of cybersecurity incident response. Decis. Support Syst. 143, 1–11.
Naseer, H., Shanks, G., Ahmad, A., Maynard, S., 2016b. Enhancing information security risk management with security analytics: a dynamic capabilities perspective. Australasian Conf. Info. Syst. 1–11.
Naseer, H., Shanks, G., Ahmad, A., Maynard, S., 2017. Towards an analytics-driven information security risk management: a contingent resource based perspective. In: Proceedings of the 25th European Conference on Information Systems, pp. 1–12.
Pan, S.L., Pee, L.G., 2020. Usable, in-use, and useful research: a 3U framework for demonstrating practice impact. Info. Syst. J. 30 (2), 403–426.
Park, Y., El Sawy, O.A., Fiss, P., 2017. The role of business intelligence and communication technologies in organizational agility. J. Assoc. Info. Syst. 18 (9), 648–686.
Phillips-Wren, G., Lakshmi, S.I., Kulkarni, U., Ariyachandra, T, 2015. Business analytics in the context of big data: a roadmap for research. Commun. AIS 37 (1), 448–472.
Ranjan, J., Foropon, C., 2021. Big data analytics in building the competitive intelligence of organizations. Int. J. Inf. Manage. 56 (102231), 1–13.
Salmela, H., Baiyere, A., Tapanainen, T., Galliers, R.D., 2022. Digital agility: conceptualizing agility for the digital era. J. Assoc. Info. Syst. 23 (5), 1080–1101.
Sarosh, P., Parah, S.A., Bhat, G.M., Muhammad, K., 2021. A security management framework for big data in smart healthcare. Big Data Res. 25, 100225.
Schilke, O., Helfat, C.E., 2018. Quo vadis, dynamic capabilities? A content-analytic review of the current state of knowledge and recommendations for future research. Acad. Manage. Annals 12 (1), 390–439.
Schultze, U., Avital, M., 2011. Designing interviews to generate rich data for information systems research. Info. Organization 21 (1), 1–16.
Shin, B., Lowry, B.P., 2020. A review and theoretical explanation of the 'cyberthreat-intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. Comput. Secur. 92, 1–16.
Simsek, Z., Vaara, E., Paruchuri, S., Nadkarni, S., Shaw, J.D., 2019. New ways of seeing big data. Acad. Manag. J. 62 (4), 971–978.
Siregar, S., Chang, K., 2019. Cybersecurity agility: antecedents and effects on security incident management effectiveness. In: Proceedings of the Twenty-Third Pacific Asia Conference on Information Systems, China, pp. 1–8.
Steininger, D.M., Mikalef, P., Pateli, A., Ortiz-De-guinea, A., 2022. Dynamic capabilities in information systems research: a critical review, synthesis of current knowledge, and recommendations for future research. J. Assoc. Info. Syst. 23 (2), 447–490.
Strauss, A., Corbin, J., 2014. Basics of Qualitative research: Techniques and Procedures For Developing Grounded Theory. Sage.
Tallon, P.P., Queiroz, M., Coltman, T., Sharma, R., 2019. Information technology and the search for organizational agility : a systematic review with future research possibilities. J. Strat. Info. Syst. 28 (2), 218–237.
Teece, D.J., Peteraf, M., Leih, S., 2016. Dynamic capabilities and organizational agility: risk, uncertainty, and strategy in the innovation economy. Calif. Manage. Rev. 58 (4), 13–36.
Teece, D.J., Pisano, G., Shuen, A., 1997. Dynamic capabilities and strategic management. Strat. Manage. J. 18 (7), 509–533.
Terzi, D.S., Terzi, R., Sagiroglu, S., 2017. Big data analytics for network anomaly detection from netflow data. In: Proceedings of the 2nd International Conference on Computer Science and Engineering, pp. 592–597.
Tseng, H.T., Aghaali, N., Hajli, D.N., 2022. Customer agility and big data analytics in new product context. Technol. Forecast. Soc. Change 180, 121690. April.
Verizon. (2022). Data breach investigations report (DBIR) 2022. https://www.verizon.com/business/resources/reports/dbir/.
von Solms, R., van Niekerk, J., 2013. From information security to cyber security. Comput. Secur. 38, 97–102.
Wang, L., Jones, R., 2021. Big data analytics in cyber security: network traffic and attacks. J. Comput. Info. Syst. 61 (5), 410–417.
Wessel, L., Baiyere, A., Ologeanu-Taddei, R., Cha, J., Jensen, T.B., 2021. Unpacking the difference between digital transformation and it-enabled organizational transformation. J. Assoc. Info. Syst. 22 (1), 102–129.
Wixom, B., Goul, M., 2014. The current state of business intelligence in academia: the arrival of big data. Commun. AIS 34 (1), 1–13.
Wong, C.K., Ahmad, A., Maynard, S.B., Naseer, H., 2020. Information security governance: a process model and pilot case study. In: Proceedings of the Forty-First International Conference on Information Systems, pp. 1–9.
Xu, L.Da, Duan, L, 2019. Big data for cyber physical systems in industry 4.0: a survey. Enterprise Info. Syst. 13 (2), 148–168.
Xu, Z., Frankwick, G.L., Ramirez, E., 2016. Effects of big data analytics and traditional marketing analytics on new product success: a knowledge fusion perspective. J. Bus. Res. 69 (5), 1562–1566.
Yeoh, W., Wang, S., Popovič, A., Chowdhury, N.H., 2022. A systematic synthesis of critical success factors for cybersecurity. Comput. Secur. 118, 1–17.

Ayesha Naseer is the member of National Cyber Security Auditing and Evaluation research group at National University of Sciences and Technology's College of Military College of Signals. She is currently working as a lecturer at MCS, NUST. Her research focuses on big data analytics, cybersecurity, incident response, and business value of data. Her research has been published in high quality journal including International Journal of Information Management.

Humza Naseer is a Lecturer at the School of Accounting, Information Systems and Supply Chain, RMIT University. He received his PhD in Management (Information Systems) from the University of Melbourne in 2019. He researches the business value of enterprise data and analytical capabilities in the context of cybersecurity, data governance, and digital transformation. Humza's work appears in the European Journal of Information Systems, Information and Organisation, Decision Support Systems, International Journal of Information Management, Journal of the Association for Information Science and Technology, Computers & Security; and conferences including the International Conference on Information Systems. Prior to returning to academia, Humza worked as a Business Analytics consultant for the Teradata Corporation. He also holds the professional designation of The Data Warehousing Institute's Certified Business Intelligence Professional with a specialization in Business Analytics..

Atif Ahmad is an Associate Professor at the University of Melbourne's School of Computing & Information Systems where he serves as Deputy Director of the Academic center of Cyber Security Excellence. Atif leads a unique team of Cybersecurity Management researchers drawn from information systems, business administration, security intelligence, and information warfare. He has authored over 100 scholarly articles in cybersecurity management and received AUD$5 M in grant funding. Atif is an Associate Editor for the leading IT security journal, Comput. Secur.. He has previously served as a cybersecurity consultant for WorleyParsons, Pinkerton and SinclairKnightMerz. Atif is a Certified Protection Professional with the American Society for Industrial Security. For more information, please visit https://www.atifahmad.me/.

Sean B. Maynard is an Associate Professor in the School of Computing and Information Systems, University of Melbourne, Australia. His-research interests are in the management of information security specifically relating to security policy, security culture, security governance, security strategy, security analytics, incident response, and privacy. He has also published in the areas of decision support systems, and business analytics. He has over eighty publications. His-research has been published in high-impact journals such as Comput. Secur., Journal of the Association for Information Science and Technology, and the International Journal of Information Management, Decision Support Systems, as well as leading conferences such as the International Conference on Information Systems. For more information, please visit https://www.seanmaynard.me/.

Adil Masood Siddiqui is an Associate Professor at the National University of Sciences and technology's (NUST) College of Military College of Signals (MCS). Adil is currently heading the Electrical Engineering Department at MCS, NUST. His-research interest includes image registration, image enhancement and defogging, risk management and cybersecurity. He has contributed over 40 research publications which include 25 high-impact factor journals.