Information & Management 58 (2021) 103392

Contents lists available at ScienceDirect

Information & Management

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

DATA BREACH MANAGEMENT: AN INTEGRATED RISK MODEL

Freeha Khan [a,1], Jung Hwan Kim [b,1,*], Lars Mathiassen [a,1], Robin Moore [a,1]

[a] J. Mack Robinson College of Business, Georgia State University, Tower Place 200, 3348 Peachtree Rd., NE Suite 500, Atlanta, GA 30326, USA
[b] Walker College of Business, Appalachian State University, 416 Howard St., NC 28608, USA

ARTICLE INFO

Keywords:
Data breach
risk management
integrated risk model
incident management
literature analysis

ABSTRACT

In response to organizations' increasing vulnerability to data breaches, we present an integrated risk model for data breach management based on a systematic review of the literature. Theoretically, the study extends the body of knowledge on data breach management by identifying and updating conceptualizations of data breach risks (items) and resolutions (actions) and by providing a foundation for organizational responses to emerging data breach incidents (heuristics). Practically, the study provides key insights that practitioners can use to organize and orchestrate effective data breach management based on comprehensive profiles of risk items and resolution techniques.

1. INTRODUCTION

Data breaches commonly involve large scale releases to external parties of sensitive data, which are regarded as important for information security [1] with their wide-ranging impacts [1–3]. For example, in 2017, Equifax announced that the sensitive information of over 145 million customers had been stolen, resulting in nearly $90 million breach-related costs from 240 consumer lawsuits [4]. According to the Ponemon Institute [5], the average total cost of data breaches in the United States reached $3.86 billion in 2018, increasing 6.4% over the previous year and covering postresponse activities such as inbound communications, investigations, remediations, and legal expenditures.

Prior studies have examined the impact of data breaches on firms' market value and stock market return [6–8], financial performance in the following year [9], and competitor behaviors within the marketplace [10]. Additionally, Goode et al. [1] suggested that organizations need to understand how their stakeholders will respond to data breaches. However, previous research provides limited insights for managing data breach incidents [11]. Therefore, there is a critical need to understand the risks of data breaches and how to effectively manage data breach incidents [11–13].

Risk management is the process of identifying and controlling vulnerabilities in information systems (IS), including risk identification, risk assessment, and risk control [14]. Baskerville et al. [15] stated that under incident-centered information security, organizations are required to manage risks by looking across past experiences to estimate future occurrences. To manage risky incidents, Lyytinen et al. [16] proposed risk management frameworks that generalize patterns of relationship between risk factors and resolution techniques to shape requisite organizational routines. Thus, a risk management perspective has been widely used in areas of IS such as software development, information security, and incident response management [14,16–19]. However, despite the increasing need for understanding data breach incidents in a risk management perspective, the literature offers few comprehensive models that integrate risks and resolutions for organizations to effectively manage data breach incidents.

To address this void, we pose the following research question: *how can organizations manage data breaches by maintaining data breach risk and resolution profiles and applying them to incidents?* To answer this question, we rely on risk management theory and a systematic review of the literature to develop an integrated risk model for data breach management. Hence, the purposes of this study are threefold: (1) to identify risks and resolution techniques based on the analysis of the literature; (2) to conceptualize the management of a data breach incident based on organizations' data breach risk and resolution profiles; and (3) to propose an integrated risk model organizations can use to respond to and learn from data breach incidents.

The paper is organized as follows. We first review and outline the literature on data breaches and risk management as the theoretical foundation underlying our study. We then adopt literature review as a

* Corresponding author.
E-mail addresses: fkahn21@student.gsu.edu (F. Khan), kimjh1@appstate.edu (J.H. Kim), lmathiassen@ceprin.org (L. Mathiassen), rmoore60@gsu.edu (R. Moore).
[1] Listed in alphabetical order as a reflection of equal authorship.

https://doi.org/10.1016/j.im.2020.103392
Received 18 July 2019; Received in revised form 31 October 2020; Accepted 14 November 2020
Available online 22 November 2020
0378-7206/Published by Elsevier B.V.

qualitative method to analyze the current literature on data breaches and risk management. Next, we synthesize the results of the analyses into an integrated model for analyzing organizations' data breach risk and resolution profiles with heuristics for managing data breach incidents. We conclude with a discussion of our contributions to theory and practice.

2. THEORETICAL BACKGROUND

2.1. Data Breaches

A *data breach* is a security incident in which sensitive, protected, or confidential data are copied, transmitted, viewed, stolen, or used by an unauthorized individual [20]. Sen and Borle [11] similarly elaborated that "sensitive, protected, or confidential data may include personal health information, personal identifiable information, trade secrets or intellectual property, and personal financial data" (p. 315). Data breaches have occurred in various industries over time, including government, healthcare, financial services, insurance, social media, and more [21]. In line with this, prior studies have been concerned with different contexts such as information technology (IT) consulting firms [22], education or healthcare organizations [23–25], and consumer markets [1,3,26] and covered both organizational [22,24] and consumer perspectives [14,27].

The impacts of data breaches are also well documented [11]. For example, Goode et al. [1] examined the effect of compensation on customer outcomes from data breaches and organizations' service recovery efforts (e.g., [27]). Kwon and Johnson [25] studied the effects of security investments in the context of data breaches under regulatory pressures. Jeong et al. [28] proposed that firms' data breaches and their IT security investments change the industry's broader security environment, which in turn, influence their competitors' proactive and reactive strategies to data breaches. Additionally, financial impacts have been researched by focusing on abnormal returns from data breaches [6, 29], security breach announcement effects on market value [9,26], financial performance [9], and stock market returns after a data breach occurred [8,30]. However, although previous research has investigated data breach impacts across industries and from different perspectives, we have limited knowledge about how organizations can identify the risks they face and develop resolution capabilities to cope with these risks. As a result, we seek to advance knowledge on data breaches based on insights from risk management theory.

2.2. Risk Management Theory

Risk management has been widely adopted in areas such as warfare, nuclear reactors, security, and financial investments [31]. Within the IS field, risk management is "the process of identifying and controlling the risks to an organization's information assets" (p. 12) [14]. In this perspective, an organization identifies vulnerabilities in its systems to protect and enhance the confidentiality, integrity, and availability of all the entities of the systems [14]. As such, risk management includes identification, assessment, and control strategies for effectively managing incidents that harm the organization.

Lyytinen et al. [16] proposed a behavioral view of risk management, drawing on rational decision and choice theory [32,33]. The behavioral view suggests managers should emphasize (1) avoiding risks of high losses [34], (2) mastering the incidents or environments to control the risks [35], and (3) making risk management a sequential pruning exercise [16]. The framework identified by Lyytinen et al. [16] sheds light on an organization's role in identifying and evaluating risks that might occur, their likelihood, and potential impacts. It also emphasizes how the organization explores and evaluates resolutions to avoid, transfer, prevent, or mitigate identified risks [16,18].

According to Lyytinen et al. [16], risk management theory focuses on three concepts: risk categories (items), resolution categories (actions), and heuristics. First, *risk categories* represent the causal dependencies between risky incidents and losses, providing the vocabulary to classify risky events and states [16]. Second, *resolution categories* refer to schematic plans for interventions that can reduce the impact of risky incidents, based on espoused causal dependencies to intervene or change the consequences of the risky incidents [16,31]. Third, *heuristics* refer to formalized decision-making routines to master environments [16] that link risk factors and resolution techniques to effectively manage risky incidents [17]. Risk categories (items) and resolution categories (actions) combined with heuristics constitute the attention shaping and intervention planning components of the risk management theory, respectively. Fig. 1 summarizes this general framing of risk management approaches.

3. RESEARCH METHOD

To advance knowledge about data breach risk management, a literature review should be complete and focus on concepts to systematically cover relevant literature on data breach and risk management [36]. Based on the structured approach by Webster and Watson [36], we implemented a six-step approach to identify relevant articles, as shown in Table 1.

We first systematically searched using Google Scholar and Business Source Complete. The former is not limited to scholarly articles and includes journals, magazines, and newspapers, whereas the latter is more specialized to scholarly journal articles. Hence, we surmised that using both databases would be appropriate to extensively find relevant articles for this study. Based on the research question and framing, we employed the following search keywords: "data breach AND risk management." As a result, we derived a total of 4,200 from Google Scholar and 1,709 articles from Business Source Complete. Because of the huge number of articles, we limited our sample to include only academic and practitioner journals, leading to 289 articles in Google Scholar and 200 articles in Business Source Complete. Out of those 489 articles, we selected 126 articles that were published in quality journals according to the criteria of SSCI (Social Science Citation Index) and SCI (Science Citation Index). After removing duplicates, we reduced the sample to 116 articles. Then, we manually read the titles and abstracts of all articles and eliminated 45 less relevant articles from the sample. Finally, following Webster and Watson's recommendations for literature reviews [36], we added 33 key articles from the references of articles selected in the previous steps. The final sample stabilized on 103 articles.

To analyze the articles, we followed the recommendations by Webster and Watson [36] to develop a conceptual framework and related coding scheme through an iterative process of refinement. We first drafted a conceptual framework and coding scheme based on risk management theory and data breach research. Through a preliminary analysis of randomly selected articles, we continued to revise and refine the coding scheme until we reached saturation (see Appendix A). Next, we conducted coder training [37]. Two of the authors independently analyzed the same sample articles. A third author who did not engage in the analysis provided oversight and assessed their codings. After each round of sample coding was complete, the three authors discussed differences in the two codings. For example, the coders had discrepancies in coding risk items because of different practical backgrounds (one is an IS security expert, and the other is a software developer). Through iterative discussions of each discrepancy in coding and how to apply the coding scheme, the three authors refined the coding scheme and the disagreements in coding decreased. Intercoder reliability can be established "by having two or more coders categorize units, and then using these categorizations to calculate a numerical index of the extent of agreement between or among the coders" (p. 590) [37]. This allowed us to assess in each iterative step how closely the two coders agreed on the coding scheme and used it consistently, including discussions of disagreements in coding, improved operationalization of the coding scheme, and increased mutual understanding between the coders. We

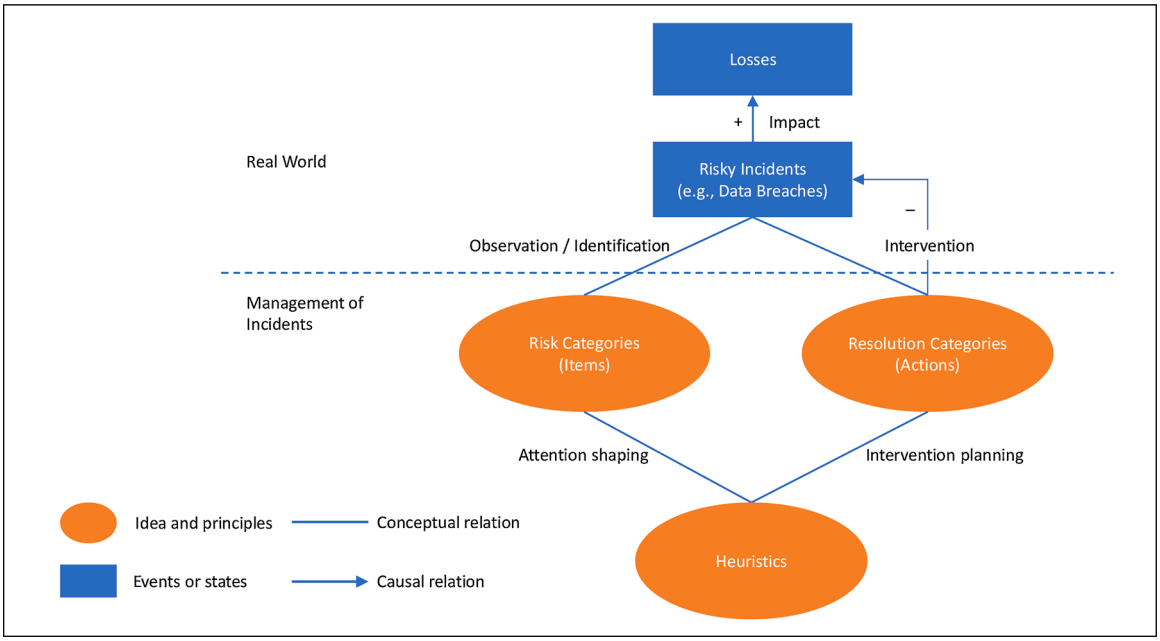

Fig. 1. Risk Management Approaches (adapted from Lyytinen et al. [16]).

Table 1
Literature Selection

Selection Step	Data Source		Sum of Articles
	Google Scholar	Business Source Complete	
Step 1: Automated search in relevant databases.	Keywords: "data breach" AND "risk management" from Google Scholar Database. We found 4,200 articles, but search limited to 500 most relevant.	Keywords: "data breach" AND "risk management" from Business Source Complete. We found 1,709 articles.	5,909
Step 2. Including only articles in academic and practitioner journals.	Result: 289 articles	Result: 200 articles	489
Step 3: Including only articles in qualified journals based on SSCI and SCI Index.	Result: 107 articles	Result: 19 articles	126
Step 4: Excluding duplicate articles.	Result: 115 articles		115
Step 5: Manually selecting relevant articles.	Result: 70 articles		70
Step 6: Adding key articles in references of selected articles.	Result: 33 articles		103

repeated this process until the intercoder reliability exceeded the recommended threshold of agreement (> 0.8). Then, the two coders split the sampled articles and independently analyzed them with the refined coding scheme.

4. CONCEPTUAL FRAMEWORK

Based on the risk management framework [16] and our review of the data breach and security literature, we propose a conceptual framework that elaborates risk categories (items), resolution categories (actions), and heuristics. The framework analyzes an organization's data breach risk and resolution profiles and subsequently applies them to manage data breach incidents, as illustrated in Fig. 2.

Lyytinen et al. [16] elaborated how risk management approaches draw on causal dependencies to control risky incidents and environments. These causal dependencies emphasize different categories of risky incidents and their losses; they are critical in identifying and assessing an organization's data breach profile. Prior studies on information security have specifically proposed risk categories of security incidents [38–40]. For example, the A⁴ Threat Model is a robust schema describing security incidents, which help organizations construct useful incident metrics from a risk management perspective [39,40]. The model focuses on the four A's of actors (whose actions affect the asset), actions (what actions affect the asset), assets (which assets are affected), and attributes (how the asset is affected), which represent the minimum information needed to describe a risky incident.

Synthesizing prior literature, we conceptualize data breach risks as follows. First, *data breach cause* is a primary event that causes a data breach incident (e.g., [41]). For instance, Sen and Borle [11] identified contextual factors influencing the risk of data breach incidents. Second, *data breach locus* is the point of adverse access to sensitive data [42]. For example, Curtin and Ayres [43] noted that data losses occur through physical assets containing sensitive data or through insider action and compromise without giving direct access to physical assets. Finally, *data breach impact* is the adverse effect a data breach incident may have on an organization [44]. As we stated, these impacts have been widely investigated in information security research.

To identify and conceptualize data breach resolutions, we draw on the incident-centered security management framework [15] that integrates the prevention and response perspectives widely used in information security management. The prevention perspective is designed to avoid security incidents from happening, whereas the response perspective is intended to react to security incidents that have occurred [15]. In particular, prior IS studies have emphasized the role of preventive controls in planning and mitigating security risks [15,45]. However, complete security risk prevention may be infeasible, such that there are increasing needs to implement effective recovery and damage control strategies for protecting organizational values following data breaches. Including proactive and reactive approaches [15], we

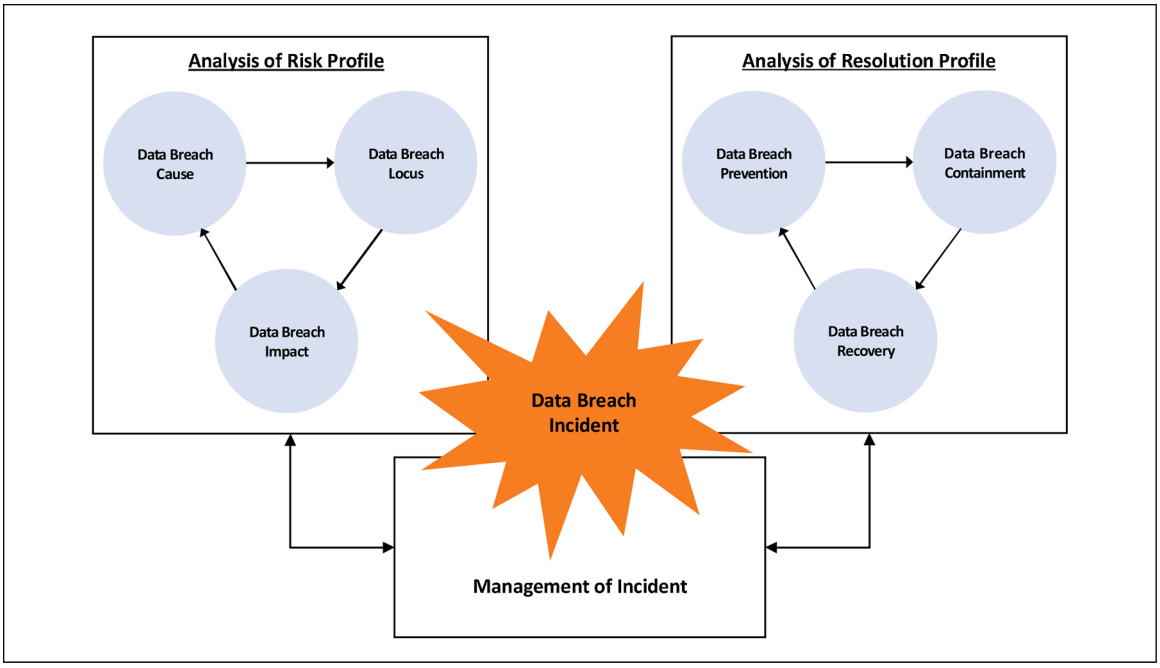

Fig. 2. Conceptual Framework.

identified three resolution categories for managing data breach risks: prevention, containment, and recovery. As a proactive category, *data breach prevention* covers interventions that are intended to lower the likelihood of a data breach and its adverse impact [15]. As reactive categories, *data breach containment* covers interventions that are intended to limit the scale and scope of a data breach immediately upon detection [14], whereas *data breach recovery* covers interventions intended to reduce the consequential adverse impact of a data breach after it occurred [14].

By analyzing organizations' risk and resolution profiles, managers can configure appropriate risk-resolutions to manage data breach incidents. Continuously drawing on these analyses and lessons from incidents, managers can then update the risk and resolution profiles to improve their risk management preparedness. In the following, we draw on risk management theory and our review of the data breach literature to elaborate these categories of risks and resolutions, as summarized in Table 2.

5. RISK CATEGORIES AND ITEMS

5.1. Data Breach Cause

Data breach cause can be categorized into intentional and unintentional data breaches. *Intentional data breaches* are incidents caused by malicious acts in which one or more humans or technology threat agents exploit vulnerabilities to cause harm to an organization [46–48]. *Unintentional data breaches* are accidental incidents caused by individuals or processes not acting with malicious intent [47–50]. As the cause is key to understanding and defending against risky security incidents, it influences the appropriate level and type of organizations' resolutions to mitigate risks. For instance, Bennett et al. [51] stated that procedural breaches, process errors, and other causes accounted for 43% of data breaches. Table 3 summarizes data breach cause categories and items.

5.1.1. Intentional Data Breach

We identified five items of intentional data breach: hackers, unauthorized access, malicious insiders, state-sponsored actors, and terrorists. *Hackers* may exploit vulnerabilities through attacks in structured query language (SQL) injection and cross-site scripting (XSS) [51] or in spyware, phishing, viruses, and scanning software [52]. *Unauthorized access* is a compromise of access control [53] or the compromised physical access of hardware such as laptops and servers [51]. *Malicious*

Table 2
Data Breach Risk and Resolution Categories.

Categories	Definitions	References
Risks:		
Data Breach Cause	The primary event that causes a data breach incident	[41]
Data Breach Locus	The point of adverse access to sensitive data	[42]
Data Breach Impact	The adverse effect a data breach may have on an organization	[44]
Resolutions:		
Data Breach Prevention	An intervention to lower the likelihood of a data breach and its adverse impact	[15]
Data Breach Containment	An intervention to limit the scale and scope of a data breach immediately upon detection	[42]
Data Breach Recovery	An intervention to reduce the consequential adverse impact of a data breach after it occurred	[37]

Table 3
Data Breach Cause Summary.

Category	Definition	Item	Reference
Intentional Data Breach	A breach incident caused by a malicious act where the intent is to cause harm to an organization	1 Hackers	[51,52]
		2 Unauthorized access	[51,53] [54,55]
		3 Malicious insiders	[56] [57]
		4 State-sponsored actors	
		5 Terrorists	
Unintentional Data Breach	A breach incident caused by accidental actions either by an individual or a process and without malicious intent	1 Insecure user behavior	[46,58] [54,59]
		2 Loss or reuse of media devices	[60,61] [12]
		3 Flawed software	[34,59]
		4 Unauthorized disclosure	
		5 Unauthorized software	

insiders constitute a significant threat to information security as they can access critical systems and data behind security measures [54]. Data breaches caused by malicious insiders range from simple access policy violations [55] to major financial fraud and theft of intellectual property [54]. Data breaches can also be caused by *state-sponsored actors*, though not generally intended to harm the public. State-sponsored actors such as the United States, Russia, Israel, and China spend considerable resources on developing threat agents and, in some cases, for a specific purpose. An example is the 2010 Stuxnet worm, which leveraged numerous unknown vulnerabilities to sabotage Iranian nuclear facilities [56]. Finally, *terrorists* may cause harm to an organization through cyberterrorism; however, they do not require access to or the removal of data to accomplish the intended harms. According to Harries and Yellowlees [57], terrorist attacks result in violence against persons or property or cause enough harm to generate fear in an organization. Unlike state sponsored actors, terrorist attacks are generally limited with a goal of making their efforts known.

5.1.2. Unintentional Data Breach

As shown in Table 3, we identified five items of unintentional data breach: insecure user behavior, loss or reuse of media devices, flawed software, unauthorized disclosure, and unauthorized software. *Insecure user behavior* includes users using weak passwords or sharing passwords; such user behaviors may be discovered while users are unaware [46,58]. *Loss or reuse of media devices* can cause unintentional data breaches due to lost paper files or media devices [51,54,59]. For example, unencrypted media devices can be a significant threat to information security systems and cause severe damages to organizations. *Flawed software* can cause data breaches unintentionally, including database vulnerabilities or faults in programming languages (e.g., vulnerabilities in IPV6, browser, and APIs) as well as vulnerable software in operating systems and applications [53,60,61]. *Unauthorized disclosure* involves inadvertent posting of sensitive information; for example, technology firms such as Google and AOL have posted customer information, which unintentionally caused data breaches [12]. The use of *unauthorized software* may disclose information through peer-to-peer file sharing [12,59]; hackers may take over a computer, sometimes thousands of them, to launch an attack on other websites [59].

5.2. Data Breach Locus

Specifically concerning breaches that result in the loss of control over sensitive data [43], it is important to identify the point (locus) of adverse access to sensitive data. Data breach locus can be categorized into physical and logical data breaches. The former is a physical point of adverse access to sensitive data [43]. The latter is a logical point of adverse access to sensitive information; this occurs when a threat agent successfully exploits a vulnerability [43,46]. The summary of data breach locus categories and items is shown in Table 4.

5.2.1. Physical Data Breach

We identified five items of loss of control over physical assets: lost paper files, stolen hardware, installed rogue devices, unauthorized physical access, and unauthorized personal computer. *Lost paper files* include lost or stolen documents, processing errors, and incorrect disposal of data [51]. Examples of process errors include hospitals accidentally mailing patient bills to the wrong patients or incorrectly disposing of paper documents. *Stolen hardware* are devices such as laptops, desktop computers, and servers with large amounts of confidential data, which are stolen and can then be accessed by an unauthorized individual [62]. *Installed rogue devices* include rogue access points, which are malicious routers attached to a secure network to gain unauthorized access to the network [61], which can then transmit records, keystrokes, websites, and screenshots back to the attacker. *Unauthorized physical access*, as mentioned earlier, can happen through the loss of physical control over assets, including hardware, laptops, or network equipment [51]. *Unauthorized personal computers* are home computers used by personnel to store corporate data. Often, these computers have little to no security measures in place, leaving them vulnerable to attack [59].

Table 4
Data Breach Locus Summary.

Category	Definition	Item	Reference
Physical Data Breach	A physical point of adverse access to sensitive data	1 Lost paper file	[51]
		2 Stolen hardware	[62]
		3 Installed rogue devices	[61]
		4 Unauthorized physical access	[51]
		5 Unauthorized personal computer	[59]
Logical Data Breach	A logical point of adverse access to sensitive data	1 Malicious software	[59,63]
		2 Vulnerable network infrastructure	[51,53]
		3 Unauthorized logical access	[46,64]
		4 Stolen intellectual property	[49,65]
		5 Flawed authorization checks	[60,66, 67]
		6 Flawed software	[60,68]

5.2.2. Logical Data Breach

We also identified six items of logical data breaches: malicious software, vulnerable network infrastructure, unauthorized logical access, stolen intellectual property, flawed authorization checks, and flawed software. *Malicious software* is any software that brings harm to the computer by spreading viruses, Trojan horses, worms, and more [59, 63]. Users may become infected by malicious software while surfing the web, through email links and attachments, or by downloading files [46]. *Vulnerable network infrastructure* allows man-in-the-middle attacks such as Internet Protocol (IP) address spoofing, Address Resolution Protocol (ARP) spoofing, Domain Name System (DNS) poisoning, Routing Information Protocol (RIP) attacks, session riding and hijacking, and flooding. For example, ARP poisoning is a well-known vulnerability in Internet protocols; there are other vulnerabilities in Internet Protocol Version 6 (IPV6), Hypertext Transfrer Protocol (HTTP), and inherent flaws in Transmission Control Protocol/Internet Protocol (TCP/IP) [46, 53]. *Unauthorized logical access* includes electronically accessing the target organization's network; that is, unauthorized individuals gain access to manage interface, customer data, employee data, or other network resources [46,64]. *Stolen intellectual property* includes breaches of software, trademark, and media exposures; intellectual capital is easily stolen in the digital age through reverse engineer products, stealing corporate secrets, or by exposing a stolen intellectual property on social media sites [49,69]. *Flawed authorization checks* include weak credential-reset mechanisms, insufficient authorization checks, or weak implementation; they allow credential interception and replay, which can make unauthorized information or actions available to hackers [46, 60,66,67]. As a result, flawed authorization checks result in infrastructure losses, large-scale session stealing, theft of identities stored in central identity management systems, and URL guessing attacks. *Flawed software* such as SQL injection attacks, command injection, cross-site scripting, and image manipulation can cause security breaches leading to lengthy unplanned downtimes, device mal-functionality, service unavailability, and large-scale information leaks [51,60,68].

5.3. Data Breach Impact

Data breaches have a variety of impacts on both individuals and organizations. The CIA (Confidentiality-Integrity-Availability) Triad Model is widely used to address the attributes of data breach incidents [70]. Adapting the model to this study, we identify three categories of data breach impacts: confidentiality, availability, and integrity. First,

confidentiality breaches are caused by data accessed outside of a business requirement [41]. Even if unintentional and with no proof data were accessed, any loss of control over the data is assumed to be a confidentiality breach. Second, *availability breaches* involve the loss of access to data or data resources for any length of time [41]. Third, *integrity breaches* are caused by unauthorized or accidental manipulation of data while at rest, in transit, or in use regardless of the parties involved [41]. Particularly, integrity data breaches are often caused by retrofitting incomplete or improperly configured technical solutions, misappropriating intellectual property and media breaches, unintentional insertion of computer viruses, or extortion to release transfer information or technology assets [49,71]. Table 5 offers a summary of data breach impact categories and items.

5.3.1. Confidentiality

We identified five adverse effects caused by confidentiality data breaches. First, *identity theft* is not always the end goal as data may be stolen without directly causing confidentiality breaches [72]. For instance, an attacker may steal the identity of a lower-level employee to gain access to data from a higher-level executive. *Fines* from data breaches resulting in the loss of confidentiality are growing [73]. For example, medical and healthcare industries have strict confidentiality rules where fines may be leveraged at the state and federal levels. *Lawsuits* come from both companies and consumers impacted by a data breach [74]. For instance, in the TJ Maxx data breach incident, the upward of 21 lawsuits were filed and cost an estimated $1 billion in recovery [63]. *Loss of competitive advantage* can be due to the loss of confidential trade secrets or customers switching to competitors after their data were stolen in a confidentiality breach [64]. *Loss of employment* may be the result of a confidentiality breach for many employees of an organization [75]. The impact to the employees would depend on the size of the organization.

5.3.2. Availability

We identified five items that cause availability data breaches. *Denial of service* is one of the most common forms of attack, typically the result of the network being flooded with unwanted data to prevent legitimate users from accessing the site or services [76]. *Stolen data* include theft of intellectual property, customer data, patient information, employee data, and any nonpublic sensitive data [64]. *Power outage* may cause systems or data to become unavailable for short amounts of time [77]. However, depending on organizations' locations, the power grip may play a significant role in the availability of the systems [78]. *System failure* is by their unplanned nature events such as software errors, human errors, and design flaws [60]. A major source of concern for organizations is malicious attackers *deleting data*. Recent attacks on data have been to encrypt data then demand a ransom, and the data will be deleted if the ransom is not paid, a practice known as ransomware [79].

Table 5
Data Breach Impact Summary.

Category	Definition	Item	Reference
Confidentiality	The adverse effect data accessed outside of a business requirement will have	1 Stolen identity	[72]
		2 Fines	[73]
		3 Lawsuits	[63,74]
		4 Loss of competitive advantage	[64] [75]
		5 Loss of employment	
Availability	Any loss of access to data or data resources for any length of time	1 Denial of service	[76] [64]
		2 Stolen data	[77,78]
		3 Power outage	[60]
		4 System failure	[79]
		5 Deleted data	
Integrity	Any unauthorized or accidental manipulation of data while at rest, in transit, or in use regardless of the parties involved	1 Modified data	[53,76, 77]
		2 Loss of competitive advantage	[64] [79]
		3 Deleted data	

5.3.3. Integrity

For integrity data breaches, we identified *data modification* as an impact of integrity data breaches that can happen by accident through human failures or disgruntled employees causing corruption, modification or the loss of information and other resources, and the interruption of services [49,53,80,81]. In addition, we identified the *loss of competitive advantage* [64] and *deleted data* [79] as impacts of integrity data breaches.

6. RESOLUTION CATEGORIES AND ACTIONS

Resolution categories include prevention (as a proactive approach), containment, and recovery (as reactive approaches). Table 6 shows the definition of each resolution category and its possible actions to manage data breach incidents in an organization.

6.1. Data Breach Prevention

Data breach prevention refers to an intervention to lower the likelihood of a data breach and its adverse impact [15]. We identified ten prevention actions as proactive responses.

The most important prevention is gaining *executive management support,* which goes beyond the approval of budgets and strategic initiatives. For instance, a culture facilitated by executive management can be a large part of data breach prevention to manage the risks [69]. *Policy and program management* is another critical aspect in the prevention of data breaches. Beyond creating and managing policies and security programs, policy and program management should be continuously reviewed, and changes need to be incorporated to improve effectiveness

Table 6
Data Breach Resolution Summary.

Category	Definition	Action	Reference
Prevention	An intervention to lower the likelihood of a data breach and its adverse impact	1 Executive management support	[54,69] [54] [57,61, 69]
		2 Policy and program management	[61]
		3 Data management	[82]
		4 Secure networks	[54]
		5 Identity and access management	[51,69] [71]
		6 Awareness and training	[83] [84]
		7 Monitoring	
		8 Benchmarking	
		9 Risk assessment	
		10 Penetration testing	
Containment	An intervention to limit the scale and scope of a data breach immediately upon detection	1 Incident detection and prevention system	[46,85] [86,87] [12,55]
		2 Computer Security and Incident Response Team	[44]
		3 Attacker tracking	
		4 Network segregation	
Recovery	An intervention to reduce the consequential adverse impact of a data breach after it occurred	1 Cybersecurity insurance	[88] [86]
		2 Computer Security and Incident Response Team	[87,89] [87,89] [51]
		3 Root cause analysis	[1]
		4 Lessons learned	
		5 Resolution before resuming operations	
		6 Response strategies	

[54]. For example, organizations need to develop security policies and protocols to review and improve access control on a regular basis. *Data management* is also a prevention measure of data breaches, including data classification [69], encryption of both data and hard drives [57], destruction of data, and the limitation of where and how data can be stored [59]. Organizations may secure mobile and media devices with encryption and make sure data are saved in the case of loss of those devices. Having a *secure network* is integral to preventing a data breach. This starts by mapping organizations' networks and resources [61]. Once mapped, any changes to the organization's networks and resources can easily be identified and investigated, making it important to continuously update the map. *Identity and access management* is the control of who an organization allows on its network or to access its applications [82]. Password length, expiration, and reuse as well as required unique usernames are important aspects of identity and access management. Regular access reviews and timely processes for the removal of access for terminated user accounts can be used for identity and access management. *Awareness and training program* is a key prevention measure to reduce accidental data breaches by employees. Awareness is an ongoing effort that includes emails, phishing campaigns, and newsletters, while training is typically driven by compliance but should recur annually [54]. *Monitoring* for data loss prevention should be conducted [69], as should the monitoring of networks, resources, awareness and training programs, and policies. Monitoring for procedural errors will allow deficiencies to be caught and new procedures to be implemented [51]. *Benchmarking* is a common practice in audit and should be included as part of an organization's compliance audit program. By conducting regular IT audits, benchmarking can be established with compliance levels to compare against [71]. *Risk assessment* should be conducted within each business unit at least annually. Organizations need to consider the relationship between systems as well as how countermeasures for one system impact other systems and their countermeasures [83]. *Penetration testing* is either internal or external to an organization, but both have the same goal, to find system vulnerabilities before they can be exploited by attackers. An internal penetration test is conducted by internal resources and has the most visibility into the systems causing the least amount of stress on the organization. An external penetration test causes the most stress on systems because its goal is to see whether it can break a system or find a way in [84]. Organizations may determine how often a penetration test is required; however, an annual test should be performed at a minimum.

6.2. Data Breach Containment

As a reactive category, *data breach containment* is an intervention to limit the scale and scope of a data breach immediately upon detection [14]. We identified four containment actions to manage data breach incidents.

Incident Detection and Prevention System (IDPS) provides the ability to identify an attack and notify appropriate personnel immediately to contain security risks. IDPS is also a useful tool for recording forensic evidence that may be used in legal proceedings against the perpetrator [85]. Identity management metrics can be helpful as well to inform how to plan the business impact, the cost to recover, and associated efforts such as notification [46]. *Computer Security and Incident Response Team (CSIRT)* "aims to minimize and contain the damage from computer security incidents, provide effective response and recovery, and help prevent future incidents. It performs some segment of the incident management activities and functions based on the organization's requirements. Incident management involves, but isn't limited to, the coverage triage and analysis, and coverage response" (p. 17) [86]. Effective and timely responses are crucial to the organization's reputation. Delayed responses not only affect the organization's standing in a negative manner but also impede other organizations' defensive and corrective measurements as the DARPA panel concluded [86]. According to Ahmad et al. [87], CSIRTs generally engage in six sequential stages: preparation, identification, containment, eradication, recovery, and follow-up. *Attacker tracking* includes the use of honeypots to track the perpetrators who are actively seeking information to commit theft [12]. Attacker tracking can be done by logging or observing a person's behavior [55]. *Network segregation* contains the affected device(s) to prevent the attack from spreading to other devices or organizations; hence, organizations need to secure their networks and may use scale-free networks [44].

6.3. Data Breach Recovery

Data breach recovery is another reactive category to reduce the consequential adverse impact of a data breach after it occurred [14]. We identified six actions of the data breach recovery category.

Cybersecurity insurance includes securing enterprises against cybersecurity risks. Regarding security investment decisions, an organization needs to understand: (1) the shape and significant input variables to its security function, (2) how to measure six input variables (effectiveness of security measures, expected number of attacks, probability of attack success, vulnerabilities, costs to organizations themselves and other parties, and payoffs for organizations themselves and other parties) that people have some decision-making authority over, and (3) whether each party has partial or complete information about the relevant variables [88]. As such, cybersecurity insurance helps organizations cover losses due to data breaches. *Computer Security and Incident Response Team (CSIRT)* provides services and support to defined constituencies—to prevent, detect, and respond to computer security incidents [86]. CSIRT provides the following services after security incidents: alerts and warnings, incident handling and analysis, incident response on site (e.g., incident response support and incident response coordination), vulnerability handling (e.g., vulnerability analysis and response, vulnerability response coordination), artifact handling (e.g., artifact analysis and response), and artifact response coordination [86]. *Root cause analysis* is used to gather evidence of misuse, identify perpetrators, and explore the methods used by perpetrators [87]. For example, the incident reports include contact details of the incident reporter, description of the identified security issues, evaluation of the sufficiency of the data, and an initial classification [89]. *Lessons learned* are analyzed after a data breach has occurred; a good security practice is to start new documentation or revise existing documentation as soon as incidents are discovered [89]. Organizations can estimate losses from comparable incidents focusing on technical lessons learned, followed by causal factors and mitigation issues [87]. Insights gained from incident responses eventually create change in security processes [87]. *Resolution before resuming operations* includes finding a solution or workaround after a data breach has occurred. Organizations should focus on any affected component to make sure that threat has been contained, and that threat will not impact any further resources [51]. For *response strategies*, organizations communicate both inside and outside once data breaches have been contained. Such communication is often a requirement, depending on the industry, state, federal, or international reporting requirements. Response strategies may reduce the impacts of data breaches and may include an apology. For instance, organizations may announce the occurrence to the public, identify how there were breaches, the containment and recovery steps taken to resolve it, and compensation plans for those affected [90]. As an effective recovery mechanism, response strategies may mitigate the consequential reputational and financial impacts of data breaches [1,45].

7. MANAGEMENT OF PROFILES AND INCIDENTS

As shown in Fig. 2, our framework proposes that organizations identify their risk and resolution profiles and link them to effectively manage data breach incidents. The proposed framework helps managers identify the profile of the data breach risks their organization faces, which enables them to develop guidelines for data breach management

in their contexts. It also helps managers prepare and respond to data breach incidents by identifying the profile of resolution techniques—prevention, containment, and recovery—that are available in their organizations. According to Baskerville et al. [15], prevention techniques aim at managing predicted threats, whereas containment and recovery techniques retain an essential role in minimizing the adverse impacts of data breaches in today's dynamic threat environments. Each resolution technique suggests a schematic plan, which decreases the likelihood and impact of risky incidents on organizations. For example, to manage unauthorized access as one of the intentional data breaches, organizations need to adopt the advanced encryption system (in prevention category), which reduces the risk of a data breach in the event of theft [51] along with secure password and authentication mechanisms [53]. As another example, to help mitigate data from being accessed on lost or stolen hardware (e.g., loss or reuse of media devices in unintentional data breach category, lost paper file and stolen equipment in physical access category, and stolen intellectual property in logical data breach category), there are two preventive measures. One is the use of disk encryption, which can be used on any hard drive that may store or process sensitive information. Another is an access control policy that not only requires a strong password but also takes action, such as deleting the data after failed password attempts.

Accordingly, our study offers guidance on how organizations can manage data breach incidents as follows. First, organizations may combine their profiles of risk and resolution categories to fit their purposes and contexts. Iversen et al. [31] suggested the risk-strategy model that links patterns of risk-resolution to outcomes. Restated, organizations assess the risk profiles with a simple scale (e.g., high or low) and classify a variety of data breach incidents in a few possible situations. For each situation, organizations build their risk strategies that are composed of appropriate resolution techniques [31,91]. In addition, specific factors such as size and subsidiary status influence the impacts of data breaches on the organization's reputation and stock market return [92]. Therefore, such risk-strategy models can help organizations manage data breach incidents contingently in uncertain contexts.

Second, rapidly changing business environments require organizations to develop dynamic capabilities that enable them to timely sense and respond to changes in the environment [93]. Organizations should appropriately and timely respond to both anticipated and unexpected changes and take advantage of change opportunities in turbulent business environments [94]. For example, the VERIS (Vocabulary for Event Recording and Incident Sharing) framework [39] can be a useful tool for evidence-based and post-incident analysis, providing metrics useful to risk management and sharing that information with others in the specific communities. To effectively manage data breach incidents, organizations need a continuous learning process focused on environmental and technological changes as well as current management capabilities. Therefore, constant vigilance in the management of data breach incidents requires organizations to keep updating their risk and resolution profiles based on lessons learned and to better respond to possible future incidents. Such organizational agility is required in today's constantly evolving data breach context.

8. DISCUSSION

Along with the increasing concerns of information security and privacy in business environments, data breaches are a key challenge to organizations. Despite numerous studies on data breaches, organizations have struggled to effectively manage data breach incidents. To address this problem, this study has developed a conceptual and practical model for data breach management from a risk management perspective and based on a systematic review of existing literature. The model offers a comprehensive conceptualization of risk categories (items) and of resolution categories (actions) as a synthesis of prior literature on data breach and risk management. Based on these insights, organizations can identify their risk and resolution profiles and draw on the implied heuristics to manage data breach incidents. As a result, we offer an integrated risk model for data breach management, as depicted in Fig. 3.

8.1. Theoretical Implications

Our study has several theoretical implications. First, we extend data breach research by offering an integrated risk model for data breach incident management. While prior studies have focused on data breach impacts in organizations, there has been little research on how organizations prevent and respond to data breach incidents [11]. Our model draws on the behavioral view of risk management, which includes risk categories and items, resolution categories and actions, and heuristics for combining them [16]. Accordingly, by synthesizing risk items and resolution techniques from prior literature, our comprehensive data breach and resolution profiles can serve as a starting point for developing different types of risk management models [31] related to data breaches in dynamic business and security environments.

Second, previous research has mostly conducted IS security management from either a prevention perspective (before data breach incidents) or a response perspective (after data breach incidents). Specifically, the prevention-oriented security frameworks and their predefined security controls have been emphasized in prior studies, even though they may be less ideal in the current dynamic threat environments [15,45]. As such, little research has integrated both perspectives to comprehensively manage data breach incidents through prevention, containment, and recovery actions. By combining two different security paradigms—prevention and response—in the data breach context, this study complements the existing body of knowledge on data breach research based on the incident-centered security management model [15].

8.2. Practical Implications

Our study also has important practical implications. First, organizations can use our conceptualization of risk-resolution profiles and the integrated approach to data breach management to shape managerial attention toward data breaches [16]. Our model allows practitioners (1) to develop risk and resolution profiles specifically to their organizational context, (2) to apply these to more effectively manage data breach incidents, and (3) to learn from these incidents to dynamically evolve their risk and resolution profiles. Through such orchestration of our integrated risk model, organizations may develop proactive and reactive heuristics and strategies [16] to manage data breach incidents.

Second, organizations are under pressure to act both swiftly and transparently to data breach incidents, as slow responses may result in legal fines and reputational damages [95]. Organizations' response time to manage data breach incidents impacts the cost of breaches beyond the data lost or disclosed. As such, the processing time to recognize, analyze, and respond to data breach incidents is vital to minimize the damages an incident may cause [86]. By identifying potential threats (i.e., risk profiles) and possible actions (i.e., resolution profiles) before an incident occurs, organizations can reduce the time it takes to respond to the incident and reduce the cost to recover from it. As such, our integrated risk model can help practitioners manage data breach incidents in a timely and cost-effective manner.

8.3. Limitations and Future Research

Researchers and practitioners should be aware of the limitations of our research. First, we followed a systematic approach to sample extant literature (Table 1). However, the reviewed articles were limited by our search keywords and criteria for including studies. For example, although we used the search keywords "data breach AND risk management," the term "data breach" is used interchangeably with security breach, privacy breach, or information breach. As such, this study may

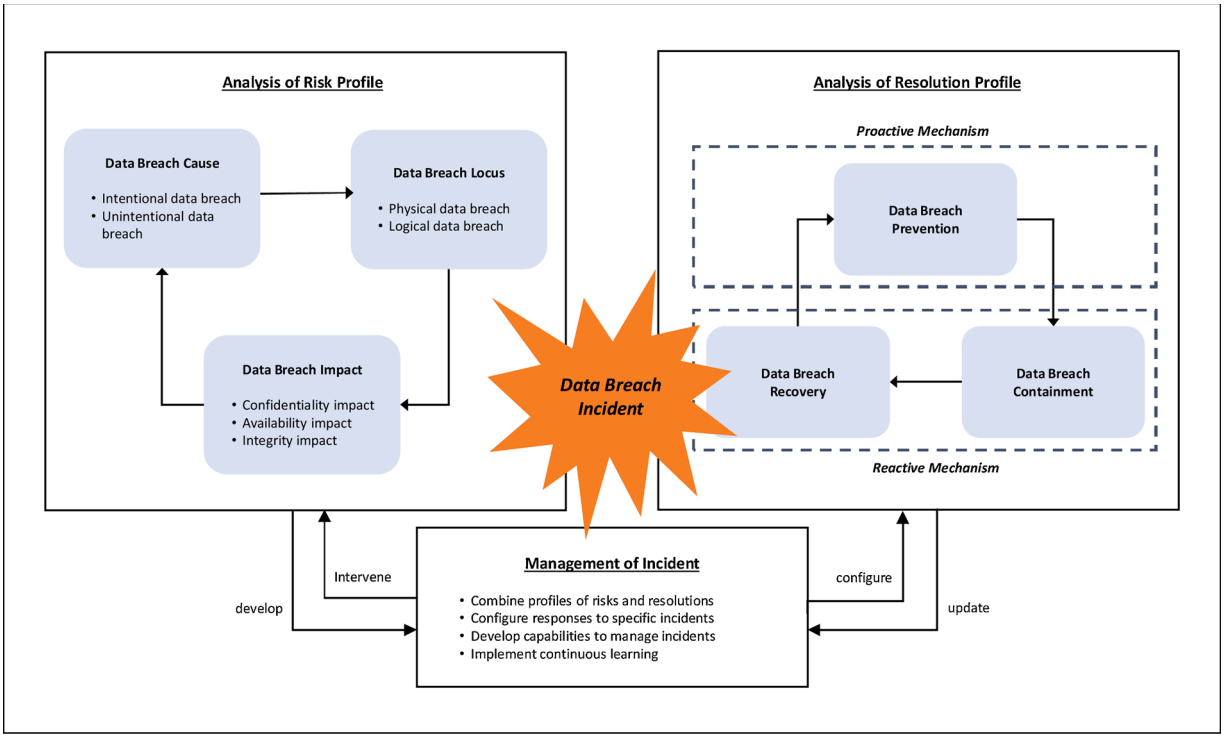

Fig. 3. Integrated Risk Model for Data Breach Management.

have omitted relevant studies that could provide further insights. For instance, Gwebu et al. [45] examined the role of response strategies in mitigating the negative financial impact of data breaches; they also argued that more nuanced response strategies are required to effectively manage data breaches. Although this study provided insights on how to manage data breaches in terms of crisis management and reputation perspectives, it was excluded from our literature sample. In addition, recent studies on information security have focused on the role of employees' compliance with IT security policies in mitigating security threats or risks [96], emphasizing that organizations can prevent data breach incidents by constantly monitoring the compliance with existing security procedures and protocols. Therefore, we encourage further research to update the proposed integrated model for data breach risk management to reduce any omission bias from excluding insights from broader literature and emerging research.

Second, the above-mentioned search criteria reveal another limitation. The management of data breach risks has been widely discussed by practitioners in business reports and practitioner journals. While those publications include valuable practical insights, we only included peer-reviewed academic articles in our sample. For example, the VERIS framework originated by Verizon's Data Breach Investigation Report (DBIR) [38,39] provides standardized metrics for reporting and sharing security incident information such as incident tracking, victim demographics, incident descriptions (the A^4 Threat Model), discovery and response, and impact assessment. These complementary insights can help organizations improve their capability to understand and manage data breach incidents. Hence, by extending the scope to include practitioner-oriented publications, future research can refine the proposed integrated risk model and reduce theory-practice gaps in the model.

Third, we did not consider the profiles of data breach risks and resolutions in specific contexts. Hence, further insights may be gained from investigating differences and commonalities across industries or firm-specific contexts. Such insights could be used to develop concrete sets risk and resolution profiles as part of risk-strategy models for specific data breach contexts.

9. CONCLUSION

In response to increasing data breach vulnerability, the present study addresses how organizations can manage data breach incidents by identifying risk and resolution profiles and by developing managerial heuristics for risk and resolution. Drawing on the risk management theory and a systematic literature review, the study provides an integrated risk model for data breach management. The model provides a foundation that researchers and practitioners can use to understand data breach incidents and to develop data breach management strategies in dynamic security environments. Specifically, the study advances research into data breach management by providing a detailed vocabulary and related heuristics for data breach risks and resolutions in light of technological developments. In doing so, it highlights the role of risk management as a comprehensive approach to constantly orchestrate data breach risks, resolutions, and heuristics in accordance with an organization's dynamic capabilities, technology architecture, and environmental changes.

CRediT authorship contribution statement

Freeha Khan: Methodology, Data curation. **Jung Hwan Kim:** Conceptualization, Methodology, Project administration, Writing - original draft, Writing - review & editing. **Lars Mathiassen:** Supervision, Conceptualization, Writing - review & editing. **Robin Moore:** Methodology, Data curation.

Appendix A. Coding Scheme

Concept	Code	Definition	Examples
Data Breach Cause	BC	The primary event that causes a data breach incident [41].	-
Intentional Data Breach	IBC	A breach incident caused by a malicious act where the intent is to cause harm to an organization [47].	Disgruntled employee who steals confidential data; hackers who breach a system to steal confidential data or cause destruction of any kind [47].
Unintentional Data Breach	UBC	A breach incident caused by accidental actions either by an individual or a process and without malicious intent [47].	Loss of media containing confidential data; accidental sharing of confidential data with unauthorized individuals by any means [47].
Data Breach Locus	BL	The point of adverse access to sensitive information [42].	-
Physical Data Breach	PBL	A breach incident caused by the loss of control over a physical asset containing sensitive information [43].	Loss of control over media of any type, or hardware such as laptops, PDAs, or other computing devices [43].
Logical Data Breach	LBL	A breach incident caused by the loss of control over logical access to sensitive information [43].	Loss of control over sensitive information through insider action(s) by an authorized employee, contractor, vendor, partner, or consumer providing access to the sensitive information whether intentional or unintentional [43].
Data Breach Impact	BI	The adverse effect a data breach may have on an organization [44].	-
Confidentiality	CBI	Data accessed outside of a business requirement whether by an authorized or unauthorized party [41].	Accessing data using electronic means such as malware, spyware, or viruses whether by a malicious actor, regardless of their being internal or external to an organization; access of confidential data by an authorized party within an organization but without a legitimate business reason [41].
Availability	ABI	Any loss of access for any length of time to data or data resources [41].	Distributed Denial of Service (DDoS) attacks causing service downtime, or unavailability of access to services or data [41].
Integrity	IBI	Any unauthorized or accidental manipulation of data while at rest, in transit, or in use regardless of the parties involved [41].	Accidental or intentional deleting of data; accidental or intentionally unauthorized altering of data; accidental or intentional unauthorized destruction of media containing data [41].
Data Breach Resolution	BR	The intervention of an organization to decrease the likelihood of a data breach or mitigate its adverse impacts [17].	-
Prevention	PBR	An intervention that is to lower the likelihood of a data breach and its adverse impacts from happening [15].	Proper warnings and safeguards (e.g., intrusion detection system, security policy, and regulation), security awareness programs, and access controls (e.g., identification, authentication, and authorization) [15].
Containment	CBR	An intervention that is to limit the scale and scope of a data breach that has happened [14].	Turning off ports or services in external organizations, cleaning up IT systems by reinstalling software [97].
Recovery	RBR	An intervention that is to reduce the adverse impacts of a data breach that has happened [14].	Disaster recovery planning for retaining or protecting information assets occurred by data breach [15].

References

[1] S. Goode, H. Hoehle, V. Venkatesh, S.A. Brown, User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach, MIS Quarterly 41 (2017) 703–727.

[2] F.K. Andoh-Baidoo, K.-M. Osei-Bryson, Exploring the characteristics of Internet security breaches that impact the market value of breached firms, Expert Systems with Applications 32 (2007) 703–725.

[3] M.J. Culnan, C.C. Williams, How ethics can enhance organizational privacy: Lessons from the ChoicePoint and TJX data breaches, MIS Quarterly 33 (2009) 673–687.

[4] S. Srinivasan, Q. Pitcher, Data breach at Equifax, Harvard Business School Publisher, 2018.

[5] Ponemon Institute, 2018 cost of a data breach study: Global overview, Ponemon Institute, 2018.

[6] H. Cavusoglu, B. Mishra, S. Raghunathan, The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers, International Journal of Electronic Commerce 9 (2004) 69–104.

[7] S. Goel, H.A. Shawky, Estimating the market impact of security breach announcements on firm values, Information & Management 46 (2009) 404–410.

[8] K. Campbell, L.A. Gordon, M.P. Loeb, L. Zhou, The economic cost of publicly announced information security breaches: Empirical evidence from the stock market, Journal of Computer Security 11 (2003) 431–448.

[9] M. Ko, C. Dorantes, The impact of information security breaches on financial performance of the breached firms: An empirical investigation, Journal of Information Technology Management 17 (2006) 13–22.

[10] H. Zafar, M. Ko, K.-M. Osei-Bryson, Financial impact of information security breaches on breached firms and their non-breached competitors, Information Resources Management Journal 25 (2012) 21–37.

[11] R. Sen, S. Borle, Estimating the contextual risk of data breach: An empirical approach, Journal of Management Information Systems 32 (2015) 314–341.

[12] M.E. Johnson, Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain, Journal of Management Information Systems 25 (2008) 97–123.

[13] P. Bromiley, M. McShane, A. Nair, E. Rustambekov, Enterprise risk management: Review, critique, and research directions, Long Range Planning 48 (2015) 265–276.

[14] M.E. Whitman, H.J. Mattord, A. Green, Principles of incident response and disaster recovery, Cengage Learning, Boston, MA, 2013.

[15] R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: Managing a strategic balance between prevention and response, Information & Management 51 (2014) 138–151.

[16] K. Lyytinen, L. Mathiassen, J. Ropponen, Attention shaping and software risk—A categorical analysis of four classical risk management approaches, Information Systems Research 9 (1998) 233–255.

[17] J.S. Persson, L. Mathiassen, J. Boeg, T.S. Madsen, F. Steinson, Managing risks in distributed software projects: An integrative framework, IEEE Transactions on Engineering Management 56 (2009) 508–532.

[18] A. Ali, D. Warren, L. Mathiassen, Cloud-based business services innovation: A risk management model, International Journal of Information Management 37 (2017) 639–649.

[19] H. Cavusoglu, H. Cavusoglu, J.-Y. Son, I. Benbasat, Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources, Information & Management 52 (2015) 385–400.

[20] U.S. Department of Health and Human Services, State and Tribal Child Welfare Information Systems, Information Security Data Breach Response Plans, Administration for Children and Families, 2015. https://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf.

[21] Breach Level Index, Data privacy and new regulations take center stage, 2018. Gemalto, https://breachlevelindex.com/request-report?thanks=1.

[22] J.V. Chen, H.-C. Li, D.C. Yen, K.V. Bata, Did IT consulting firms gain when their clients were breached? Computers in Human Behavior 28 (2012) 456–464.

[23] J.D. Collins, V.A. Sainato, D.N. Khey, Organizational data breaches 2005-2010: Applying SCP to the healthcare and education sectors, International Journal of Cyber Criminology 5 (2011) 794–810.

[24] C.M. Angst, E.S. Block, J. D'arcy, K. Kelley, When do IT Security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches, MIS Quarterly 41 (2017) 893–916.

[25] J. Kwon, M.E. Johnson, Proactive versus reactive security investments in the healthcare sector, MIS Quarterly 38 (2014) 451–471.

[26] O. Hinz, M. Nofer, D. Schiereck, J. Trillig, The influence of data theft on the share prices and systematic risk of consumer electronics companies, Information & Management 52 (2015) 337–347.

[27] A. Malhotra, C.K. Malhotra, Evaluating customer information breaches as service failures: An event study approach, Journal of Service Research 14 (2011) 44–59.

[28] C.Y. Jeong, S.-Y.T. Lee, J.-H. Lim, Information security breaches and IT security investments: Impacts on competitors, Information & Management 56 (2019) 681–695.

[29] K. Kannan, J. Rees, S. Sridhar, Market reactions to information security breach announcements: An empirical analysis, International Journal of Electronic Commerce 12 (2007) 69–91.

[30] L.A. Gordon, M.P. Loeb, L. Zhou, The impact of information security breaches: Has there been a downward shift in costs? Journal of Computer Security 19 (2011) 33–56.

[31] J.H. Iversen, L. Mathiassen, P.A. Nielsen, Managing risk in software process improvement: An action research approach, MIS Quarterly 28 (2004) 395–433.
[32] K. Arrow, Aspects of the theory of risk-bearing, Helsinki, Finland, 1965.
[33] J. Yates, Risk-taking behavior, John Wiley & Sons, Chichester, 1992.
[34] R.M. Cyert, J.G. March, A behavioral theory of the firm, Prentice-Hall, Englewood Cliffs, NJ, 1963.
[35] K. Maccrimmon, D.A. Wehrung, Taking risks: The management of uncertainty, Free Press, New York, 1986.
[36] J. Webster, R.T. Watson, Analyzing the past to prepare for the future: Writing a literature review, MIS Quarterly 26 (2002) xiii–xxiii.
[37] M. Lombard, J. Snyder-Duch, C.C. Bracken, Content analysis in mass communication: Assessment and reporting of intercoder reliability, Human Communication Research 28 (2002) 587–604.
[38] G.B. Moreira, V.M. Calegario, J.C. Duarte, A.F.P. dos Santos, Extending the VERIS framework to an incident handling ontology, IEEE/WIC/ACM International Conference on Web Intelligence (WI) (2018) 440–445.
[39] W. Baker, M. Goudie, A. Hutton, C.D. Hylender, J. Niemantsverdriet, C. Novak, D. Ostertag, C. Porter, M. Rosen, B. Sartin, 2011 data breach investigations report, Verizon RISK Team, 2011. https://www.wired.com/images_blogs/threatlevel/2011/04/Verizon-2011-DBIR_04-13-11.pdf.
[40] W.H. Baker, Toward a decision support system for measuring and managing cybersecurity risk in supply chains, Ph.D. Dissertation, Virginia Tech, 2017.
[41] M. Benaroch, A. Chernobai, J. Goldstein, An internal control perspective on the market value consequences of IT operational risk events, International Journal of Accounting Information Systems 13 (2012) 357–381.
[42] T.N. Wall, J.A. Hayes, Depressed clients' attributions of responsibility for the causes of and solutions to their problems, Journal of Counseling Development 78 (2000) 81–86.
[43] C.M. Curtin, L.T. Ayres, Using science to combat data loss: Analyzing breaches by type and industry, 2009. Interhack, http://web.interhack.com/publications/interhack-breach-taxonomy.pdf.
[44] C.D. Huang, R.S. Behara, Q. Hu, Managing risk propagation in extended enterprise networks, IT Professional (July/August) (2008) 14–19.
[45] K.L. Gwebu, J. Wang, L. Wang, The role of corporate reputation and crisis response strategies in data breach management, Journal of Management Information Systems 35 (2018) 683–714.
[46] B. Grobauer, T. Walloschek, E. Stocker, Understanding cloud computing vulnerabilities, IEEE Security & Privacy 9 (2011) 50–57.
[47] I.H. Elifoglu, I. Abel, Ö. Taşseven, Minimizing insider threat risk with behavioral monitoring, Review of Business 38 (2018) 61–73.
[48] J. Meszaros, A. Buchalcevova, Introducing OSSF: A framework for online service cybersecurity risk management, Computers & Security 65 (2017) 300–313.
[49] C. Biener, M. Eling, J.H. Wirfs, Insurability of cyber risk: An empirical analysis, The Geneva Papers 40 (2015) 131–158.
[50] M. Ramachandran, V. Chang, Towards performance evaluation of cloud service providers for cloud data security, International Journal of Information Management 36 (2016) 618–625.
[51] K. Bennett, A.J. Bennett, K.M. Griffiths, Security considerations for e-mental health interventions, Journal of Medical Internet Research 12 (2010) 1–11.
[52] I. Cook, S. Pfleeger, Security decision support challenges in data collection and use, IEEE Security & Privacy 8 (2010) 28–35.
[53] C. Modi, D. Patel, B. Borisaniya, A. Patel, M. Rajarajan, A survey on security issues and solutions at different layers of cloud computing, Journal of Super Computing 63 (2013) 561–592.
[54] Z.A. Soomro, M.H. Shah, J. Ahmed, Information security management needs more holistic approach: A literature review, International Journal of Information Management 36 (2016) 215–225.
[55] A. Vance, P.B. Lowry, D. Eggett, Using accountability to reduce access policy violations in information systems, Journal of Management Information Systems 29 (2013) 263–290.
[56] A. Aleem, A. Wakefield, M. Button, Addressing the weakest link: Implementing converged security, Security Journal 26 (2013) 236–248.
[57] D. Harries, P.M. Yellowlees, Cyberterrorism: Is the US healthcare system safe? Telemedicine and e-Health 19 (2013) 61–66.
[58] S. Spiekermann, L.F. Cranor, Engineering privacy, IEEE Transactions on Software Engineering 35 (2009) 67–82.
[59] M.J. Culnan, E.R. Foxman, A.W. Ray, Why IT executives should help employees secure their home computers, MIS Quarterly Executive 7 (2008) 49–56.
[60] K. Hole, L.-H. Netland, Toward risk assessment of large-impact and rare events, IEEE Security & Privacy 8 (2010) 21–27.
[61] J. Hale, P. Brusil, Secur(e/ity) management: A continuing uphill climb, Journal of Network Systems Management 15 (2007) 525–553.
[62] R. Ogie, Bring your own device: An overview of risk assessment, IEEE Consumer Electronics Magazine 5 (2016) 114–119.
[63] J.J. Ryan, T.A. Mazzuchi, D.J. Ryan, J.L. De la Cruz, R. Cooke, Quantifying information security risks using expert judgment elicitation, Computers & Operations Research 39 (2012) 774–784.
[64] A.A. Yayla, Q. Hu, The impact of information security events on the stock value of firms: The effect of contingency factors, Journal of Information Technology 26 (2011) 60–77.
[65] E. Andrijcic, B. Horowitz, A macro-economic framework for evaluation of cyber security risks related to protection of intellectual property, Risk Analysis 26 (2006) 907–923.
[66] E. Paintsil, Evaluation of privacy and security risks analysis construct for identity management systems, IEEE Systems Journal 7 (2013) 189–198.
[67] N. Zahadat, P. Blessner, T. Blackburn, B.A. Olson, BYOD security engineering: A framework and its analysis, Computers & Security 55 (2015) 81–99.
[68] K. Fu, J. Blum, Controlling for cybersecurity risks of medical device software, Communications of the ACM 56 (2013) 35–37.
[69] M.E. Johnson, E. Goetz, S.L. Pfleeger, Security through information risk management, IEEE Security & Privacy 7 (2009) 45–52.
[70] S. Samonas, D. Coss, The CIA strikes back: Redefining confidentiality, integrity and availability in security, Journal of Information System Security 10 (2014) 21–45.
[71] N. Thompson, R. Ravindran, S. Nicosia, Government data does not mean data governance: Lessons learned from a public sector application audit, Government Information Quarterly 32 (2015) 316–322.
[72] W. Roberds, S.L. Schreft, Data breaches and identity theft, Journal of Monetary Economics 56 (2009) 918–929.
[73] S.E. Goodman, R. Ramer, Global sourcing of IT services and information security: Prudence before playing, Communications of the Association for Information Systems 20 (2007) 812–823.
[74] W. Xu, G. Grant, H. Nguyen, X. Dai, Security breach: The case of TJX companies, Inc, Communications of the Association for Information Systems 23 (2008) 575–590.
[75] C. Posey, T.L. Roberts, P.B. Lowry, R.T. Hightower, Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders, Information & Management 51 (2014) 551–567.
[76] A. Dutta, G.C.A. Peng, A. Choudhary, Risks in enterprise cloud computing: the perspective of IT experts, Journal of Computer Information Systems 53 (2013) 39–48.
[77] R. Clarke, Data risks in the cloud, Journal of Theoretical and Applied Electronic Commerce Research 8 (2013) 59–73.
[78] M.E. Paté-Cornell, M. Kuypers, M. Smith, P. Keller, Cyber risk management for critical infrastructure: a risk analysis model and three case studies, Risk Analysis 38 (2018) 226–241.
[79] C.S. Kruse, B. Frederick, T. Jacobson, D.K. Monticone, Cybersecurity in healthcare: A systematic review of modern threats and trends, Technology and Health Care 25 (2017) 1–10.
[80] A. Shameli-Sendi, R. Aghababaei-Barzegar, M. Cheriet, Taxonomy of information security risk assessment (ISRA), Computers & Security 57 (2016) 14–30.
[81] J. D'Arcy, S. Devaraj, Employee misuse of information technology resources: Testing a contemporary deterrence model, Decision Sciences 43 (2012) 1091–1124.
[82] G. Peterson, Introduction to identity management risk metrics, IEEE Security & Privacy 4 (2006) 88–91.
[83] V. Viduto, C. Maple, W. Huang, D. LóPez-PeréZ, A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem, Decision Support Systems 53 (2012) 599–610.
[84] J.L. Bayuk, Security as a theoretical attribute construct, Computers & Security 37 (2013) 155–175.
[85] A. Patel, M. Taghavi, K. Bakhtiyari, J.C. JúNior, An intrusion detection and prevention system in cloud computing: A systematic review, Journal of Network Computer Applications 36 (2013) 25–41.
[86] R. Ruefle, A. Dorofee, D. Mundie, A.D. Householder, M. Murray, S.J. Perl, Computer security incident response team development and evolution, IEEE Security & Privacy 12 (2014) 16–26.
[87] A. Ahmad, S.B. Maynard, G. Shanks, A case analysis of information systems and security incident responses, International Journal of Information Management 35 (2015) 717–723.
[88] R. Rue, S.L. Pfleeger, Making the best use of cybersecurity economic models, IEEE Security & Privacy 7 (2009) 52–60.
[89] I.A. Tøndel, M.B. Line, M.G. Jaatun, Information security incident management: Current practice as reported in the literature, Computers & Security 45 (2014) 42–57.
[90] T. Wang, K.N. Kannan, J.R. Ulmer, The association between the disclosure and the realization of information security risk factors, Information Systems Research 24 (2013) 201–218.
[91] L. Mathiassen, T. Tuunanen, M. Rossi, T. Saarinen, A contingency model for requirements development, Journal of the Association for Information Systems 8 (2007) 569–597.
[92] K.M. Gatzlaff, K.A. McCullough, The effect of data breaches on shareholder wealth, Risk Management and Insurance Review 13 (2010) 61–83.
[93] D.J. Teece, G. Pisano, A. Shuen, Dynamic capabilities and strategic management, Strategic Management Journal 18 (1997) 509–533.
[94] S.H. Haeckel, Adaptive enterprise: Creating and leading sense-and-respond organizations, Harvard Business Press, 1999.
[95] R. Sobers, Data breach response times: Trends and tips, 2020. https://www.varonis.com/blog/data-breach-response-times/.
[96] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, MIS Quarterly 34 (2010) 523–548.
[97] R. Werlinger, K. Muldner, K. Hawkey, K. Beznosov, Preparation, detection, and analysis: The diagnostic work of IT security incident response, Information Management & Computer Security 18 (2010) 26–42.

Freeha Khan is a senior software engineer with Dell Technologies and doctoral student at Georgia State University with emphasis on cloud computing. She has also been an adjunct professor at the Kennesaw State University. In the practical field, she manages the cloud hosting application and works with cross functional teams to ensure the security, compliance, and automation needs required for the application. She has more than twenty

years of experience in the information technology field. She has a Bachelor of Science in Computer Science and Masters in Information Systems from the Kennesaw State University.

Jung Hwan Kim is an assistant professor of CIS in the Walker College of Business at the Appalachian State University. He received his doctorate from Georgia State University. His research focuses on digital innovation, on information security and risk management, and on emergent technologies. His research has appeared in the *Decision Support Systems, Data Base for Advances in Information Systems, International Journal of Information Management, Journal of Computer Information Systems, Journal of Consumer Marketing, Journal of Global Information Management,* and conference proceedings in premium IS conferences.

Lars Mathiassen is a Georgia Research Alliance Eminent Scholar, professor at the Computer Information Systems Department, and cofounder of The Center for Process Innovation at Georgia State University. His research focuses on the development of software and information services, on IT-enabled innovation of business processes, and on the management and facilitation of organizational change processes. He has published extensively in major information systems and software engineering journals and has coauthored several books on the subject, such as Professional Systems Development, Computers in Context: The Philosophy and Practice of Systems Design, Object Oriented Analysis & Design, and Improving Software Organizations: From Principles to Practice. He has served as a senior editor for MISQ, and he currently serves as the senior editor for Information & Organization and for the Journal of Information Technology.

Robin Moore is an adjunct professor in the computer information systems (CIS) department at the Georgia State University and a senior information security engineer at Change Healthcare. His teaching interests focus on cybersecurity, security audit, and compliance. With over a decade of IT security experience covering physical security, application security, security auditing, compliance, and vendor management, he holds the CISSP and CEH certifications as well as BS and MS degrees in information systems focused in cybersecurity along with a doctorate of business administration (DBA). His research focuses on behavioral information security.