12-12-2020

Really, What Are They Offering? A Taxonomy of Companies' Actual Response Strategies after a Data Breach

Till Diesterhöft

Kristin Masuch

Maike Greve

Simon Trang

Really, What Are They Offering? A Taxonomy of Companies' Actual Response Strategies after a Data Breach

Till Diesterhöft[1]
University of Goettingen,
Goettingen, Lower Saxony, Germany

Kristin Masuch
University of Goettingen,
Goettingen, Lower Saxony, Germany

Maike Greve
University of Goettingen,
Goettingen, Lower Saxony, Germany

Simon Trang
University of Goettingen,
Goettingen, Lower Saxony, Germany

ABSTRACT

Data breaches have become an everyday phenomenon. As a consequence, organizations no longer solely focus on prevention but also proactively prepare for the next data breach. A key element of these efforts is data breach response strategies that aim to retain trust and loyalty of the affected parties. Prior research provides important insights into the effects, causes, and conditions of effective response strategies. However, an underlying conceptualization of different forms of data breach response strategies is lacking. By analyzing the response strategies of 313 data breaches, we inductively derive a taxonomy of data breach response strategies. Our results suggest that response actions can be classified along eight dimensions including 22 distinct characteristics. Our research provides contributions to research and practice. The taxonomy provides a comprehensive framework and allows to link different research streams logically. Subsequently, the taxonomy helps managers to distinguish different data breach response strategies and implement suitable measures.

[1] Corresponding author. tillole.diesterhoeft@uni-goettingen.de +49 (0)551 / 39-21704

Keywords: data breaches, response strategies, response actions, taxonomy, affected companies

INTRODUCTION

In recent years, a cross-industry rise in data breaches has been observed (Identity Theft Resource Center 2019; Sen and Borle 2015). Since such incidents often cause severe negative consequences for the affected companies, such as deterioration of customer relationships (Choi et al. 2016; Goode et al. 2017), loss of customer trust (Culnan and Williams 2009), and a decline in stock market value (Campbell et al. 2003; Malhotra and Kubowicz Malhotra 2011), companies focus on various costly proactive measures to prevent data breaches. However, previous research has shown that security incidents are not entirely preventable (Sen and Borle 2015); hence, companies should pay increasing attention to reactive measures (Goode et al. 2017). However, these strategies are manifold (Gwebu et al. 2018) and are often chosen quickly by the affected companies (Otto et al. 2007). Even the security literature shows an ambivalent picture in response research. Several studies focus on single response actions such as compensation (Goode et al. 2017; Gwebu et al. 2018) and apology (Gwebu et al. 2018; Masuch et al. 2019). However, it is noticeable that the authors define such strategies differently and hence do not cover the same spectrum of response strategies (e.g., Bitner (1990); Fehr and Gelfand (2010); Masuch et al. (2019)). This, in turn, leads to difficulties in transferring and comparing research results. Therefore, it is necessary to create a common understanding of the different response strategies and their components. Since much of the literature is dealing with apology and compensation, the diversity of response strategies (Gwebu et al. 2018) has not yet received sufficient coverage. In this respect, it is necessary to investigate response strategies in practice and depict them in a comprehensible way to provide researchers with additional examination possibilities. Thus, a much broader investigation of response strategies can be

facilitated than it is in the current state. Moreover, due to new legislation in Europe, it is now mandatory for companies to inform their customers about data breaches (Council of the European Union 2016) and thus prepare a data breach response strategy. An investigation of actual response strategies would support companies in designing their data breach response strategy and reveal configuration possibilities. To address the practical problem of companies to develop a suitable response strategy and the research problem of an unstructured landscape of post-breach behavior, our research aims to classify actual data breach response strategies to provide an overview of possible strategies and their definitions.

Our research approach covers two different aspects. On the one hand, the actual data breach response strategies of companies must be examined. Thus, strategies discussed in the literature are reviewed and adjusted if necessary. In addition, it is possible that other strategies not covered in the literature may be identified. In turn, this has the effect of creating a common understanding. It also encompasses finding an answer to the classification of these constructs. The creation of a classification leads to an increased comprehension regarding the composition of them. Identifying different strategies and classifying them will contribute to the literature that will support the scientific community to understand data breach response strategies and their structure better. The classification technique of taxonomy is used in this paper to create a data breach response strategy taxonomy. The development process is based on a comprehensibly generated data set of 313 different data breaches to incorporate companies' actual strategies. The taxonomy development method of Nickerson et al. (2013) is followed and adapted in some parts.

BACKGROUND ON DATA BREACH RESPONSE STRATEGIES

A data breach is a security incident in which data is intentionally or unintentionally exposed to an unauthorized third party (Cheng et al. 2017). Previous research has shown that a

data breach's effects are reflected in the affected company's stock value. In general, it has been found that data breaches harm the stock value because they are adverse events that indicate that the company is being abused (e.g., Cavusoglu et al. (2004), Gatzlaff and McCullough (2010), Garg et al. (2003)). The recent literature states that the data breach itself and the company's response have an impact on the stock price (Masuch, Greve, and Trang 2020). Another particular problem is that customers may perceive the company and its performance as inadequate after a data breach (Parasuraman et al. 2005), which can harm its reputation and where response actions become an unavoidable corporate strategy (Goel and Shawky 2009). Similarly, the responses of the companies and the response actions they contain will strongly influence the customers' perspective (Weiner 2001). These strategies should restore customer confidence and stabilize their relationship with the company (Goode et al. 2017). Research on data breach response actions already includes several studies that analyze the impact of company responses on customer behavior (e.g., Goode et al. (2017); Greve et al. (2020)). This literature evaluates which strategies can positively influence customer behavior. Studies generally focus on two main strategies, apology and compensation (e.g., Goode et al. (2017); Masuch, Greve, Cyrenius, et al. (2020)). While some apology aspects are sometimes included in the notification of customers after a breach, an especially complementary effective response action is to compensate affected customers (Goode et al. 2017). Research has shown that compensation has a positive effect on the customer's attitude, and thus adverse effects can be reduced (e.g., Ettredge and Richardson (2003)). Thus, this stream of research also informs the present paper. It becomes clear that the existing literature has already investigated the effects of single specific response actions after a data breach. However, there is a fundamental lack of a common understanding of which response actions exist and are used.

METHODOLOGICAL APPROACH

Data breaches must first be identified, which are then used as the basis for analysis to develop a data breach response strategy taxonomy. Table 1 shows our research approach with these two phases.

Table 1. Research Approach

	Phase 1: Data Breach Collection	**Phase 2: Taxonomy Development**
Steps	• Search for data breaches in existing databases • Filtering of non-analyzable data breaches	• Specification of meta-characteristics • Define ending-conditions • Iterative identification of response strategy dimensions and characteristics
Method	Structured search of data breaches	Taxonomy development method (Nickerson et al. 2013)
Source	EbscoHost, ProQuest, WiSo, Privacy Rights Clearinghouse	Data breach collection (Phase1)
Results	Identification of 313 data breaches	8 Dimensions with a total of 22 characteristics

Phase 1: Data Breach Collection

To derive a data breach collection, we conducted a structured search of data breaches (see figure 1). Sources for potential data breaches included public as well as literature databases. We started with "Privacy Rights Clearinghouse," a public database for security incidents, and received 306 cases.

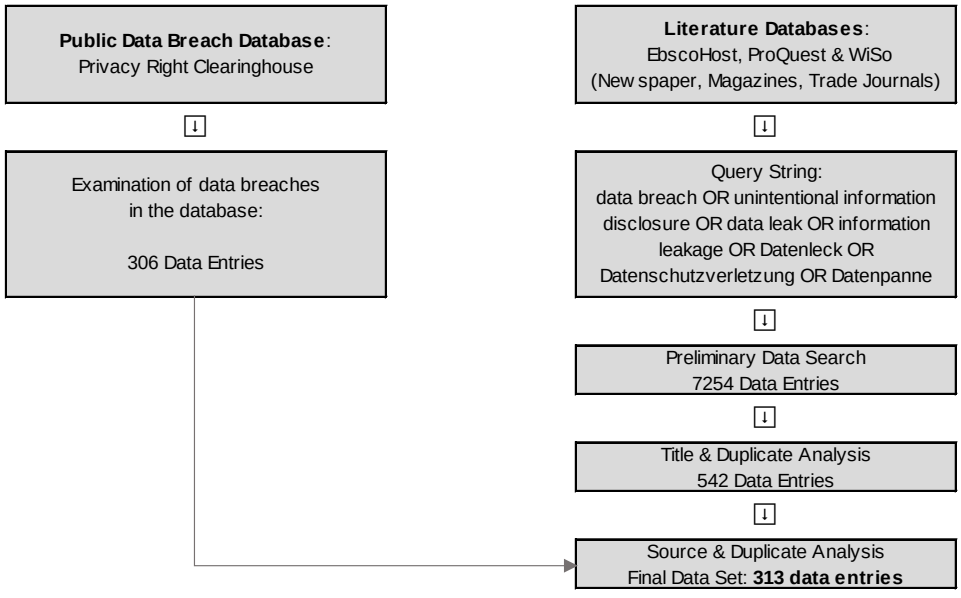

Figure 1: Structured Search of Data Breaches

As a second source, we then examined newspapers, magazines, and trade journals in several literature databases. This led to a total of 542 data breaches following title and duplicate analysis. Both data sets were joined and checked for the availability of sources, duplicates were removed again. A data breach was declared with a positive availability if all messages of a company published within a period of 30 days were still accessible. The chosen interval is justified by the field-related service failure literature (Goode et al. 2017), which identifies this period as the largest relevant time period to measure an impact on the market value (Malhotra and Kubowicz Malhotra 2011). This resulted in a final data set containing 313 data breaches that are allocated between 2001 and 2020. The search was carried out in March 2020 and resulted in an aggregated total of 313 data breaches.

Phase 2: Taxonomy Development

Nickerson et al. (2013) taxonomy development method was designed application area independent and has been applied to various research domains in the information systems context (e.g., Haas et al. (2014); Nakatsu et al. (2014); Prat et al. (2015)). In addition to the broad utilization of the methodology, the formalization of process steps facilitates an objective comprehensibility of the developed taxonomy and improves transferability of research results. Moreover, the method offers a differentiation between empirical derivation and conceptual verification of characteristics, supporting the suitability of its application to address our problem statement. Additionally, it is the only taxonomy development method we are aware of that exists within the field of information systems. Although there are taxonomy methods from other fields of research, e.g. phenetics (Sokal and Sneath 1963) or cladistics (Eldredge and Cracraft 1980), these are not described concretely but rather provide a very abstract explanation. Therefore, we consider Nickerson et al.'s (2013) method to be the most suitable for our research. Since we

defined the data basis initially before the taxonomy development and not in an ad-hoc manner, as in the case of Nickerson et al. (2013), the method has to be modified to these circumstances (see figure 2).

The goal of the taxonomy development method is to create a taxonomy that "[…] must be explanatory, not descriptive […]" (Nickerson et al. 2013, p. 346). In the first step, the meta-characteristics have to be defined as they highly influence the results of the emerging taxonomy and indicate the utilization scope of a taxonomy (Nickerson et al. 2013).

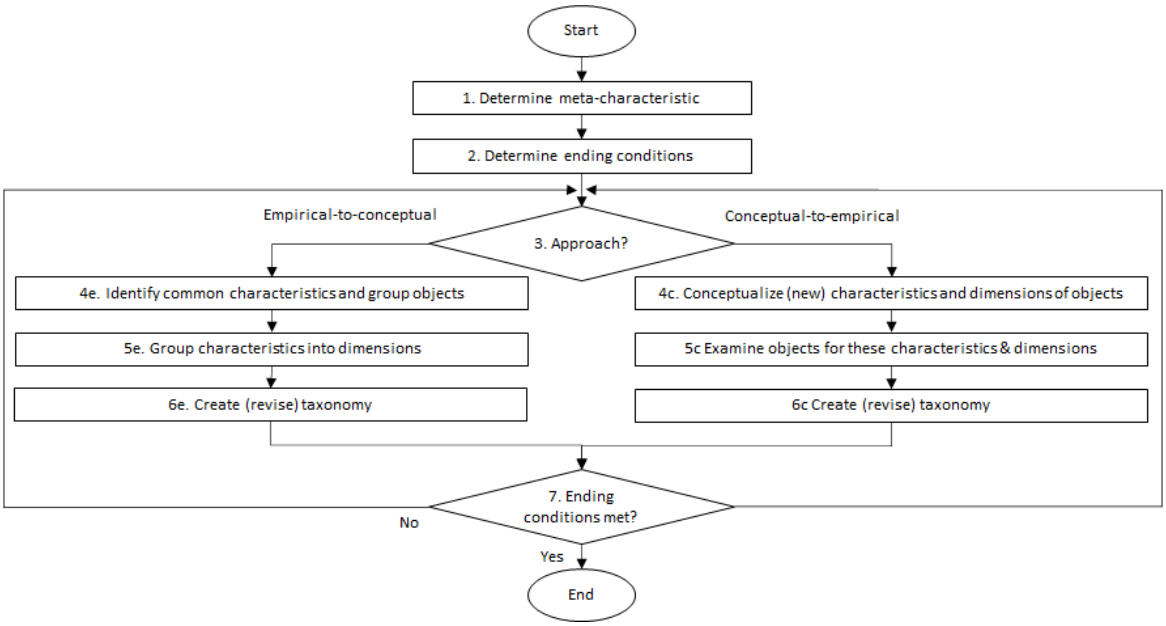

Figure 2. Taxonomy Development Method (adapted from Nickerson et al. 2013)

We analyze only publicly available data. Hence, the resulting taxonomy contains reactions that have been revealed through communication with the public. This leads to the definition of the meta-characteristic:

(controllable) reactions revealed by communication between the company and the public after the occurrence of a data breach.

By this definition, it can be conceptualized that the resulting data breach response strategy taxonomy does not consist of different strategies but rather of strategy components

(characteristics). This assumption is based on the fact that a taxonomy possesses several characteristics that can be combined in any possible way (Nickerson et al. 2013). Next, due to the taxonomy development model's iterative nature, conditions are defined that represent an endpoint for the development process. Because the examined objects were identified beforehand and are thus not a part of the taxonomy development itself, Nickerson et al.'s (2013) first two objective ending conditions referring to the iterative manipulation of objects are not suitable. This is justified by the fact that the data search is considered exhaustive in its scope, and therefore all objects were identified. Additionally, duplicate and source analyses were performed, leading to the assumption that a later removal of objects is not necessary. The other remaining five objective and subjective conditions are adopted in their entirety (see Nickerson et al. (2013)). Instead of identifying new objects, characteristics are identified within the existing database. This leads to a more comprehensible identification of characteristics. In turn, to ensure an exhaustive development process, an additional objective ending condition must be added. This is defined as follows: The examined data set may not show any indications of new characteristics.

RESULTS

We initiated the taxonomy development with a conceptual-empirical iteration, identifying dimensions and characteristics from the existing literature. Afterward, an empirical-conceptual iteration was performed to complement those. The two following iterations were conducted empirically. The fifth iteration checked if all ending conditions are met to complete the taxonomy. In total, five iterations were performed. An overview is shown in figure 3.

The first iteration is based on data breach literature. This led to identifying six recurrent dimensions of response strategies, which have a total of 14 characteristics (see figure 3). First,

the compensation dimension was identified. Based on the literature, compensation can be provided by a service or monetary reward. Gwebu et al. (2018), for example, are oriented towards compensation through exclusive credit monitoring service and Goode et al. (2017) towards compensation through products and services. Masuch, Greve, and Trang (2020) define compensation as payment, either material or immaterial, reflecting the monetary component.

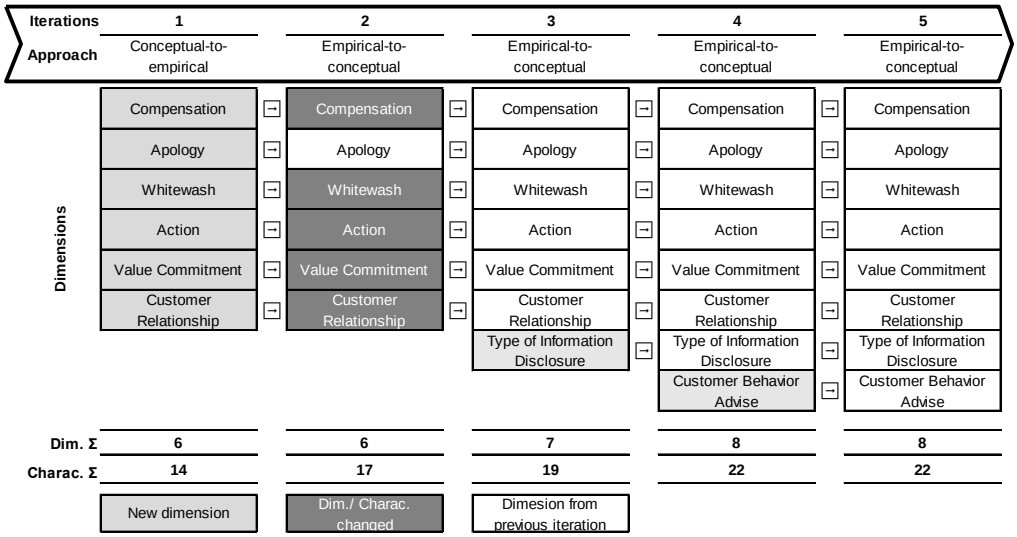

Figure 3. Data Breach Response Taxonomy Building Process– Iterative Development of Dimension Selection

In addition, another characteristic of the dimension compensation was empirically-conceptually identified in the second iteration. It was found that in the actual reactions of companies to a data breach, the combination of service and monetary compensation also exists (see iteration 2). The second dimension identified in the data breach literature is the apology. It has the characteristics where a company may or may not apologize for the data breach to the customer (Masuch, Greve, and Trang 2020). The third dimension is the whitewashing of a data breach. Here the company downplays the situation and is much more positive about it than it is (Masuch, Greve, Cyrenius, et al. 2020). In addition to the literature-based definition, the statements of companies show that they also whitewash by denying the breach or highlighting

previous positive actions of the organization (see iteration 2). The fourth dimension that emerges from the data breach literature is what a company took or promises to take to correct the data breach (Gwebu et al. 2018). According to the literature, the actions can be proactive or preventive (Gwebu et al. 2018). Proactive refers to measures that have already been taken, and preventive refers to actions implemented to prevent the data breach from reoccurring. Furthermore, stating the successful (re)provision of services or products is encompassed under the proactive characteristic. Empirically, the combination of the two can be determined, which can be described as comprehensive. The fifth dimension that can be identified is the commitment to value. Gwebu et al. (2018) describe it as a part of the strategy type image renewal, which focuses on the breached company's values. An example is the promise to protect security and privacy is mentioned (Gwebu et al. 2018). In the statements, a supplement can also be found for this dimension. In their responses to a data breach, companies often address the value of transparency in addition to security (see iteration 2).

Table 2. Practical Examples of the Dimensions for the First and Second Iteration

Iteration 1 + 2	
Dimensions [Characteristics]	**Practical Examples**
Compensation [monetary & service]	*"[…] offering a "Welcome Back" package […]. This will include, among other benefits, a month of free PlayStation Plus membership for all PSN customers, as well as an extension of subscriptions for PlayStation Plus and Music Unlimited customers […]"* (Sony 2011a)*) & "[…] enrollment in an identity theft protection program."* (Sony 2011b)
Apology [apology]	*"We sincerely regret and deeply apologize for any inconvenience or concern that this may have caused you"* (Toyota Motor Coporation 2016)
Whitewash [whitewash]	*"[…] that may have subjected your personal information, including your name, address, date of birth, Social Security number, and income to unauthorized access. Even though we believe that it is highly unlikely that this information has been used without authorization […]"* (Summit Financial Group Inc. 2015).
Action [preventive]	*"[…] worked with the shipping company and payment processing bank to ensure that this type of loss cannot occur again […] "* (Marriott 2011).
Value Commitment [security]	*"[…] the security of your transactions, documents and data are our top priority"* (DocuSign 2017).
Customer Relationship [focused]	*"[…] appreciate all of our loyal customers through the decades"* (Rutter's 2020).

The sixth dimension that has been added from the data breach literature is the relationship with the customer. Gwebu et al. (2018) note that companies attempt to make those affected like them. To do so, the company mentions the relationship with its customers in a positive sense (Gwebu et al. 2018). Moreover, it can be empirically identified that affected organizations indicate that

their customers are the highest priority or that customers generally come first (see iteration 2). Table 2 shows practical examples for the dimensions created in the first and second iteration.

The third iteration is based exclusively on the response strategies found in the data set. Thereby another dimension could be identified empirically, the type of information disclosure. This can be open or secret. Companies using an open type of information disclosure provide a comprehensive amount of information about the data breach. In contrast, the secret response type is without or with few and incomplete information. Practical examples of the dimensions added in the third and fourth iteration can be found in table 3.

Table 3. Practical Examples of the Dimensions for the Third and Fourth Iteration

Iteration 3 + 4	
Dimensions [characteristics]	**Practical Examples**
Type of Information Disclosure [open]	*"[…] accounts were compromised by a very targeted attack on user names, passwords and security questions […]"* (Apple 2014).
Customer Behavior Advise [recommendations]	*"[…] recommend that patients regularly review the explanation of benefits that they receive from their health insurer"* (21st Century Oncology 2016).

The fourth iteration, which is also conducted empirically, adds another dimension. In the data, the dimension of behavioral advice for customers was identified. Using this dimension, companies give their customers recommendations on how to behave after the data breach to avert, minimize, or detect the damage early on. In addition, the provision of supplementary, unspecified information is encompassed by this dimension (e.g., through call centers).

Table 4. Dimensions and Characteristics of Data Breach Response Taxonomy

Dimensions	**Characteristics**			
Compensation	monetary (0)	service (151)	monetary and service (8)	none (154)
Apology	apology (229)		none (84)	
Whitewash	whitewash (280)		none (33)	
Action	proactive (139)	preventive (10)	comprehensive (115)	none (49)
Value Commitment	security (188)	transparency (8)	security and transparency (56)	none (61)
Customer Relationship	focused (107)		not focused (206)	
Type of Information Disclosure	open (257)		secretly (56)	
Customer Behavior Advise	recommendations (280)		none (33)	

Legend:	Conceptual Dimension & Characteristics	Empirical Dimension & Characteristic	Empirical Characteristic	Empirically extended Characteristic

Note: The numbers in the brackets indicate the number of data breaches that show these characteristics.

In the fifth and last iteration, it is verified whether the taxonomy's ending conditions are met or if further adaptations are needed. It can be determined that all conditions are met. Thus, the development process can be completed. An overview of the final dimensions and their characteristics is displayed in table 4.

DISCUSSION

Contribution to Literature

This research contributes to the data breach and data breach response strategy literature. Firstly, we collected a unique data set of data breaches and their response strategies. Due to the traceable creation of the data set, the content is reproducible and facilitates an improved scientific discussion. The collected information enabled the construction of a taxonomy and can also be used for quantitative analysis in the future. Overall, it offers new research opportunities and provides knowledge about response strategies implemented by companies.

Secondly, we contribute to the literature by developing the taxonomy and the associated classification of organizations' data breach response strategies. It allows the still new research area to gain a fundamental overview of possible strategies that can be performed. Thus, leading to an enhancement of the current response strategy knowledge. Thereby, the existing findings of different authors are summarized and empirically tested, but also completely new strategy components are identified through taxonomy development. In this context, it is also worth noting that the terminology of strategy, which is widely used in the literature, has been subdivided into strategy dimensions and characteristics for better differentiation and classification. This definition provides an in-depth look at data breach response strategies and their composition. The various possibilities of strategies, which result from the combination of the individual

characteristics, enable unprecedented research possibilities and the generation of new knowledge in the field of data breaches.

Thirdly, selective strategy dimensions were created, allowing later researchers to orient themselves on these definitions. In turn, this leads to establishing a common understanding within the scientific community and supports the scholarly discussion about data breach response strategies. Because each dimension and characteristic has undergone an empirical examination, it is based not only on conceptualization but on an empirically validated manner.

Practical Implications

Besides the contribution to literature, our study holds several implications for practice. Firstly, the developed taxonomy allows companies to compare their strategy with those of competitors. This enables organizations to see the dimensions of their own data breach response strategy and how other affected companies are responding to a data breach. This contribution represents a novelty that supports and extends the companies' view on data breaches and data breach response strategies. Secondly, new research possibilities arise, which are highlighted in the next chapter. When analyses are conducted on newly identified dimensions and their impact on market value, customer loyalty or costs, companies can ultimately benefit by adopting the strategy that promises to yield the greatest effect on these parameters. This can increase the efficiency and effectiveness of an organizations' data breach response strategy. This contribution will only be realized at a later stage and is dependent on future research; it is noted here because the developed taxonomy paved the way for the mentioned potential benefits.

Limitations and Opportunities for Future Research

This study has important limitations, which must be regarded when examining and utilizing the results. However, this work itself and its limitations offer opportunities for future

researchers. The first limitation arises from the application of Nickerson et al.'s (2013) taxonomy development method. Even if a rigorous following of the adapted method has been carried out, the findings obtained by the respective processes are shaped by subjectivity. However, the results of these processes were evaluated by two authors. Nevertheless, the proportion of subjectivity is reduced by an objective decision-making process; there remains a residual subjectivity. This should be considered when studying the individual dimensions and characteristics, especially those derived empirically. The second limitation is that a company's response strategy to show no reaction to a data breach (Bansal and Zahedi 2015) cannot be included in the taxonomy because it contradicts the rules of taxonomy building (Nickerson et al. 2013). No response to the data breach cannot be used in combination with other identified response strategies. The third limitation concerns the development of the dimensions itself. In our paper, only the content of companies' responses to data breaches was considered for taxonomy development. Future research could look at other aspects besides the content of the companies' published responses, such as time aspects, like the speed of disclosure, or context-specific aspects, like the publication format. The fourth limitation of this work relates to the type of data breaches investigated. Only data breaches that have been disclosed by a public announcement are included in the underlying data set. This is because there was no access to internal information. In turn, this leads to the conclusion that an application of the taxonomy is especially useful for public data breach response strategies. Moreover, it must be said that the examined data breaches are predominantly attributable to US American companies and primarily affect consumer-related data (87.5%). The data breaches were mostly caused by malicious third parties (68%). The five industries with the largest number of data breaches are retail, financial services, technology, hospitality, and health. The average company size is of around 65000 employees.

The development of the data breach response strategy taxonomy enables future researchers and practitioners to apply it in different contexts. Only through these applications, the actual usefulness can be realized and verified. Subsequent research should analyze the identified data set qualitatively and quantitatively, e.g., cluster analysis or text mining. This could lead to a higher information density of characteristics and dimensions, which could result in an overall better utility of the taxonomy. It is also advisable to focus not only on the outcomes themselves but also identifying how such strategies are planned, by whom they are executed, and how companies select strategy components. This knowledge could be utilized to extend the data breach response strategy taxonomy.

CONCLUSION

This study deals with developing a taxonomy of the actual response strategies of companies after a data breach. It is based on 313 responses to data breaches. A total of 8 dimensions, encompassing 22 characteristics, from the literature and the company responses could be identified. The developed taxonomy offers further potential for future research, which can be taken from the text above. Furthermore, the data breach response taxonomy provides a consistent foundation and overview of companies' response strategies, which are used in theory and practice.

REFERENCES

21st Century Oncology. 2016. *Security Incident*. (https://web.archive.org/web/20160415154712/https://www.21co.com/SecurityIncident), accessed May 10, 2020.

Apple. 2014. *Apple Media Advisory*. (https://www.apple.com/newsroom/2014/09/02Apple-Media-Advisory/), accessed March 15, 2020.

Bansal, G., and Zahedi, F. M. 2015. "Trust Violation and Repair: The Information Privacy Perspective," *Decision Support Systems* (71), pp. 62–77.

Bitner, M. J. 1990. "Evaluating Service Encounters: The Effects of Physical Surroundings and Employee Responses," *Journal of Marketing* (54:2), p. 69.

Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. 2003. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market*," *Journal of Computer Security* (11:3), pp. 431–448.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. "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* (9:1), pp. 70–104.

Cheng, L., Liu, F., and Yao, D. D. 2017. "Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* (7:5), pp. 1–14.

Choi, B. C. F., Kim, S. S., and Jiang, Z. 2016. "Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior," *Journal of Management Information Systems* (33:3), pp. 904–933.

Council of the European Union. 2016. "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016," *European Parliament*.

Culnan, and Williams. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly* (33:4), p. 673.

DocuSign. 2017. *DocuSign Trust Center | Personal Safeguards*. (https://web.archive.org/web/20170610042418/https://trust.docusign.com/en-us/personal-safeguards/), accessed June 07, 2020.

Eldredge, N., and Cracraft, J. 1980. *Phylogenetic Patterns and the Evolutionary Process*, New York: Columbia University Press.

Ettredge, M. L., and Richardson, V. J. 2003. "Information Transfer among Internet Firms: The Case of Hacker Attacks," *Journal of Information Systems* (17:2), pp. 71–82.

Fehr, R., and Gelfand, M. J. 2010. "When Apologies Work: How Matching Apology Components to Victims' Self-Construals Facilitates Forgiveness," *Organizational Behavior and Human Decision Processes* (113:1), Elsevier Inc., pp. 37–50.

Garg, A., Curtis, J., and Halper, H. 2003. "Quantifying the Financial Impact of IT Security Breaches," *Information Management & Computer Security* (11:2), pp. 74–83.

Gatzlaff, K. M., and McCullough, K. A. 2010. "The Effect of Data Breaches on Shareholder Wealth," *Risk Management and Insurance Review* (13:1), pp. 61–83.

Goel, S., and Shawky, H. A. 2009. "Estimating the Market Impact of Security Breach Announcements on Firm Values," *Information and Management* (46:7), pp. 404–410.

Goode, S., Hoehle, H., Venkatesh, V., and Brown, S. A. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach," *MIS Quarterly* (41:3), pp. 703–727.

Greve, M., Masuch, K., and Trang, S. 2020. "The More, the Better? Compensation and Remorse as Data Breach Recovery Actions – An Experimental Scenario-Based Investigation," in *WI2020 Zentrale Tracks*, GITO Verlag, pp. 1278–1293.

Gwebu, K. L., Wang, J., and Wang, L. 2018. "The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management," *Journal of Management Information Systems* (35:2), pp. 683–714.

Identity Theft Resource Center. 2019. *Multi-Year Data Breach Chart*. (https://www.idtheftcenter.org/wp-content/uploads/2019/02/Multi-Year-Chart.pdf), accessed February 21, 2020.

Malhotra, A., and Kubowicz Malhotra, C. 2011. "Evaluating Customer Information Breaches as Service Failures: An Event Study Approach," *Journal of Service Research* (14:1), pp. 44–59.

Marriott. 2011. *Important Security and Protection Notification*. (https://www.doj.nh.gov/consumer/security-breaches/documents/marriott-vacation-club-20110131.pdf), accessed July 13, 2020.

Masuch, K., Greve, M., Cyrenius, J., Wimmel, B., and Trang, S. 2020. "Do I Get What I Expect? An Experimental Investigation of Different Data Breach Recovery Actions," in *Twenty-Eight European Conference on Information Systems (ECIS 2020)*, pp. 1–18.

Masuch, K., Greve, M., and Trang, S. 2019. "Does It Meet My Expectations? Compensation and Remorse as Data Breach Recovery Actions-An Experimental Scenario Based Investigation," in *Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy*, pp. 1–15.

Masuch, K., Greve, M., and Trang, S. 2020. "Please Be Silent? Examining the Impact of Data Breach Response Strategies on the Stock Value," in *Forty-First International Conference on Information Systems (forthcoming) (ICIS 2020)*, pp. 1-17.

Nickerson, R. C., Varshney, U., and Muntermann, J. 2013. "A Method for Taxonomy Development and Its Application in Information Systems," *European Journal of Information Systems* (22:3), pp. 336–359.

Otto, P. N., Antón, A. I., and Baumer, D. L. 2007. "The Choicepoint Dilemma," *IEEE Security and Privacy* (5:5), pp. 15–23.

Parasuraman, A., Zeithaml, V. A., and Malhotra, A. 2005. "E-S-QUAL a Multiple-Item Scale for Assessing Electronic Service Quality," *Journal of Service Research* (7:3), pp. 213–233.

Rutter's. 2020. *Notice of Payment Card Incident*. (https://web.archive.org/web/20200215134143/https://www.rutters.com/paymentcardincident/), accessed March 20, 2020.

Sen, R., and Borle, S. 2015. "Estimating the Contextual Risk of Data Breach: An Empirical Approach," *Journal of Management Information Systems* (32:2), pp. 314–341.

Sokal, R. R., and Sneath, P. 1963. *Principals of Numerical Taxonomy*, San Francisco, CA: W.H. Freeman and Company.

Sony. 2011a. *News: Consumer Alerts*. (https://web.archive.org/web/20110427094959/http://us.playstation.com/news/consumeralerts/), accessed May 23, 2020.

Sony. 2011b. *Sony Offering Free `AllClear ID Plus' Identity Theft Protection in the United States through Debix, Inc.* (https://blog.playstation.com/2011/05/05/sony-offering-free-allclear-id-plus-identity-theft-protection-in-the-united-states-through-debix-inc/), accessed May 23, 2020.

Summit Financial Group Inc. 2015. *Data Security Incident.* (https://oag.ca.gov/system/files/Sample%20Notice%201_0.pdf), accessed June 20, 2020

Toyota Motor Coporation. 2016. *Notice of Data Breach*. (https://oag.ca.gov/system/files/2008%20--%20CUSTOMER%20Letter%20for%20AG_0.pdf), accessed June 20, 2020

Weiner, B. 2001. "Reflections and Reviews Attributional Thoughts about Consumer Behavior," *Journal of Consumer Research* (27:December 2000), pp. 382–387.