# Show-and-Tell or Hide-and-Seek? Examining Organizational Cybersecurity Incident Notifications

W. Alec Cram
University of Waterloo
wacram@uwaterloo.ca

Rissaile Mouajou-Kenfack
University of Waterloo
rmouajoukenfack@uwaterloo.ca

## Abstract

*The growing frequency of cybersecurity incidents commonly requires organizations to notify customers of ongoing events. However, the content contained within these notifications varies widely, including differences in the level of detail, apportioning of blame, compensation, and corrective action. This study seeks to identify patterns contained within cybersecurity incident notifications by constructing a typology of organizational responses. Based on a detailed review of 465 global cybersecurity incidents that occurred during the first half of 2020, we obtained and qualitatively analyzed 187 customer notifications. Our results reveal three distinct organizational response types associated with the level of detail contained within the notification (full transparency, guarded, opacity), as well as three additional response types associated with the benefitting party (customer interest, balanced interest, company interest). This work extends past classifications of cybersecurity incident notifications and provides a template of possible notification approaches that could be adopted by organizations.*

## 1. Introduction

Cybersecurity incidents are increasingly common within organizations [1, 2] and often require communications with customers regarding details of the event [3, 4]. These notifications can come in various forms, including formal press releases, postings on company websites, emails, social media, and blogs. Stakeholders, including shareholders, governments, regulators, and the media, pay close attention to organizational responses to cybersecurity incidents in determining what actions they may wish to take [5, 6].

Although past research has established the link between cybersecurity incidents and downstream consequences on stock prices [7-9], management turnover [10], and audit fees [11], there has been a limited focus on the actual content contained within publicly available cybersecurity incident notifications. Depending on the country where the organization is based, as well as the nature of the incident itself, these notices can include acknowledgements of what occurred, what systems/data were impacted, and what the organization is doing (or has done) to respond. Although basic notification templates are available from a variety of sources [e.g., 12, 13, 14], no widely accepted format has yet been established and the nature of communications can vary widely [3, 15]. Recent work on the topic has begun to investigate the relationships between the individual choices made by organizations (e.g., offering compensation or apologizing) and how these choices can impact customers [e.g., 16, 17] and investors [e.g., 18].

However, the details contained within cybersecurity incident notifications are particularly important to customers and provide valuable signals regarding the organization's priorities and managerial philosophy. Past research suggests that stakeholders (including customers, employees, the media, and the legal system) make judgements on an organization's properties and behaviors, which combine to form macro-level conclusions about the legitimacy of the institution; these perceptions can directly influence performance and access to resources [5]. In a cybersecurity incident context, we argue that the content included in a notification to customers can serve to shape how those customers judge if an organization's response is fair and reasonable. Such judgements could then contribute to downstream actions, such as diminished market share, regulatory penalties, and lawsuits.

In order to investigate this further, we pose the following research question: *What patterns are present in the approaches used by organizations when notifying customers about cybersecurity incidents?* To address this question, we examined the organizational responses to 465 global cybersecurity incidents reported between January and June 2020. From these, we collected 187 incident notifications and qualitatively analyzed their content. We identified three distinct organizational response types associated with the "level of detail" contained within the notification, as well as three additional response types associated with the "benefitting party".

Our results contribute to the cybersecurity literature by articulating the distinct approaches that organizations use when responding to cybersecurity incidents.

URI: https://hdl.handle.net/10125/80165
978-0-9981331-5-7

Although past research has classified the individual characteristics of organizational responses, we are not aware of past research that has grouped these characteristics together to form higher level response categories. The development of these categories is an important step in analyzing the resulting downstream stakeholder consequences and can be leveraged by managers when determining the optimal strategy for communicating cybersecurity incident details to customers. We also provide a distinctly global view on cybersecurity incident notifications, which stands in contrast to much past research that commonly focuses on U.S.-based incidents.

The remaining sections of our paper are presented as follows. First, we describe the conceptual background, in terms of the crisis response strategies used by organizations. Next, we outline our methodological approach, including data collection and analysis. We then present our results, discuss the implications for research and practice, and conclude with opportunities for future research.

## 2. Conceptual background

Broadly, cybersecurity refers to "the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems" [19, p. 41]. Within organizations, an important element of a successful cybersecurity management program is effectively responding to incidents, which represent unexpected events that could compromise business operations [20].

In framing our study, we draw on concepts from the marketing, organizational behavior, and information systems literature related to how institutions respond to emergency situations. In doing so, we consider the different approaches and strategies that can be adopted. Of particular interest in this study are the approaches used to communicate with customers following cybersecurity incidents. Although organizations may need to communicate (e.g., risk disclosures) with other stakeholders such as regulators or investors based on formalized guidelines [21-23], our interest in customer notifications is motivated by the flexibility that many organizations have in how much or how little to disclose following an incident. In cases where private customer information is compromised, organizations may be required to meet at least a minimum standard of notification procedures, but these guidelines vary depending on the location of the incident [24]. However, firms may choose to offer more details than necessary. On the one hand, many organizations are sensitive to the inconvenience that cybersecurity incidents can have on customers and are keen to express regret for the role they may have played in the event; on the other hand, organizations are wary of the legal and financial difficulties that may result from formally accepting responsibility for an incident. We provide an overview of these crisis response strategies in the following section, which forms an important basis for our analysis.

### 2.1. Crisis response strategies

Past research suggests that customers are acutely aware of the events and behaviors displayed by the organizations they interact with, which can lead to either satisfying or unsatisfying experiences [25]. In the specific context of a crisis situation, which refers to "an untimely but predictable event that has actual or potential consequences for stakeholders" [26, p. 64], how an organization responds can have long-term impacts on its reputation and profitability [27].

A key element of an organization's response to a crisis pertains to its communications with stakeholders. Indeed, "managing a crisis effectively is crucial in reestablishing control of the organization, restoring the company image, and regaining stakeholder trust" [28, p. 164]. For example, organizational apologies following a crisis have been found to correspond with inconsistent results. Some research suggests that leaders who apologize for mistakes are perceived positively by victims [29], while other others perceive apologies as reinforcing views of unfairness, particularly in cases where the communication is viewed as insincere [30].

The effectiveness of an organization's response to a crisis can be evaluated in a variety of ways. Past research has pointed to the reactions of customers on social media [31], the consistency of communications over time [32], and proactive preparations that can overcome crisis barriers [33] as factors associated with effective responses.

### 2.2. Responses to cybersecurity incidents

In the context of cybersecurity incidents, which we view as a type of organizational crisis (per the definition provided above), a good deal of research attention has been dedicated to the financial consequences of cybersecurity incident announcements. For example, Cavusoglu et al. [7] evaluate the link between data breach announcements and the market value of the announcing firm. Similarly, Malhotra and Malhotra [34] examine the links between reports of data breaches and a decline in the market value of a firm.

More recently, research has extended beyond treatments of incident announcements as a binary, "black box" and increasingly consider the nature and characteristics of the announcement itself. For example, Masuch et al. [18] evaluate the consequences of firm response strategies after a data breach. The results suggest that apologizing after a data breach has detrimental effects on investor behavior, while whitewashing (i.e., downplaying the incident) has a small positive effect on stock value. Similarly, Diesterhöft et al. [15] analyze the response strategies of 313 data breaches and derive a taxonomy from the results, including compensation, apology, whitewashing, action, value commitment, customer relationship, type of information disclosure, and customer behavior advice. Other work by Greve et al. [17] evaluates the link between a company's recovery actions (i.e., compensation or remorse) and a customer's satisfaction. The study finds that a mix of both compensation and remorse is best to increase customer satisfaction, but that severe data breaches limit the positive benefits that remorse can have on satisfaction. Finally, Goode et al. [35] consider how much compensation to offer customers following a cybersecurity incident. Results from the study indicate that compensating customers can have a positive impact on perceived service quality and intentions to continue as a customer.

Cultural differences can also play a role in the consequences of a cybersecurity incident. For example, Greve et al. [16] compare customer satisfaction levels in Germany and Bolivia following data breaches. The study examines the impact of compensation or an apology, as well as the broader implications on loyalty, trust, and word of mouth. The authors find that that cultural differences do exist, such as Germans being more likely to demand compensation, while Bolivians tend to be satisfied with an apology. Similarly, Kim and Lee [36] compare organizational statements pertaining to cybersecurity incidents from firms located in the United States and South Korea. They find differences in terms of responsibility admittance and expressions of sympathy (more South Korean firms contained these elements), as well as with reassurance and compensation (more U.S. firms contained these elements).

## 2.3. Research approach

Based on the background described above, our objective in this study was to build on past research that identifies the typical characteristics of cybersecurity incident notifications to better understand how those characteristics are aggregated together. Although managers are undoubtedly aware of the potential benefits and drawbacks of specific customer response tactics (e.g., apologizing or offering compensation), it remains unclear how organizations assemble collections of tactics together to form a notification strategy. Although we might expect managers to select several notification characteristics that align with the context, risk, and objectives of the firm, the existing research has not yet uncovered the extent to which patterns may exist in the characteristics of cybersecurity notifications.

We suggest that this line of inquiry can provide important insights into the broader strategies and techniques used by organizations in response to cybersecurity incidents. From a practice perspective, identifying such patterns can provide clarity on the alternative approaches that could be adopted as a response to cybersecurity incidents. From a research perspective, identifying relationships between notification characteristics is a key step in constructing broader theoretical connections between incident response approaches and subsequent downstream impacts, such as diminished market share, regulatory penalties, and lawsuits. Although we confine our focus in this study to the patterns within incident notifications, we view this as an important step towards uncovering downstream relationships with these important outcomes of interest. We outline the details of our methodological approach in the following section.

# 3. Methodology

We adopted a qualitative, content analysis approach based on publicly available information associated with cybersecurity incidents. This approach was deemed appropriate since we were interested in the characteristics and content contained within the cybersecurity notifications made by organizations. Although the Privacy Rights Clearinghouse database has been commonly used in past research related to cybersecurity incidents [e.g., 37, 38, 39], at the time the study was conducted, no data had been published related to 2020 incidents. As a result, we chose to draw on a listing of worldwide cybersecurity incidents published by IT Governance Ltd. [40]. Each month, the website publishes a listing of links to publicly announced cybersecurity incidents, including ransomware attacks and data breaches, from around the world.

We focused on the incidents reported by the website during January through June 2020. This period was chosen because it provided a lengthy list of incidents and allowed for several months to elapse following each incident (our data collection was conducted in the first quarter of 2021), which would provide sufficient time for organizations to craft and release incident notifications to customers. We identified a total of 465 incidents (61 in January, 105 in February, 62 in March, 48 in April, 103 in May, and 86 in June). For each incident, we recorded the company name, date that the incident was reported, industry, type of incident, a summary of the incident, and details of the organizational response. Where this information was incomplete based on the initial link provided by the IT Governance website, we conducted supplementary searches in three databases—ABI/INFORM, Factiva, and Nexis Uni—using keywords such as "breach", "incident", and "cyberattack" alongside the company name. We also searched each organization's website for cybersecurity incident notifications. A total of 187 incident notifications were identified.

We arrived at several explanations as to why some of the identified incidents did not have notifications. First, depending on the date of the incident, some notifications may have been released on a corporate website and then subsequently taken offline before our research was conducted. In other cases, notifications may not have been created because the incidents did not directly affect customer data or occurred in countries where notifications were not required. Finally, depending on the nature of the organization (e.g., defense administrations, educational institutions), incident notifications were sometimes sent via traditional mail or email and were not posted online.

### 3.1. Data analysis

Our data analysis focused on the 187 collected cybersecurity incident notifications. We qualitatively analyzed the content of the notifications based on a series of nine characteristics drawn from the crisis response and cybersecurity literature (refer to Table 1). Although we do not claim that the listed characteristics are exhaustive, we intended to draw on a thorough collection of the characteristics identified in past research (see references in Table 1 for coding sources).

For each of the notifications, we recorded whether the corresponding characteristics were present or absent. During the coding process, the author team met regularly to discuss the coding approach. Where there were any ambiguities in determining a particular incident's characteristics, the author team discussed the situation and agreed on a coding outcome.

**Table 1. Coding Characteristics**

| **Notification Characteristic** | **Definition** |
|---|---|
| Detailed explanation | Recognition that a cybersecurity event has occurred, as well as the articulation of specific details (e.g., what happened, when it occurred). |
| Whitewashing | Diverting blame away from the victim organization and blaming others (e.g., employees, suppliers); also includes downplaying of the severity of the incident [15, 18]. |
| Apology | An expression of remorse or regret about the incident [18, 41]. |
| Compensation | The offering of monetary (e.g., refunds or discounts) or service (e.g., credit monitoring) compensation to customers impacted by the incident [15, 35, 41]. |
| Responsive action | A description of the proactive and/or preventive actions that have been (or will be) undertaken by the organization in the wake of the incident [15]. |
| Value commitment | Explanation of the company's commitment to ensuring security and/or transparency [15]. |
| Focused on the customers | Explicit recognition of the importance of customers to the company [15]. |
| Open information disclosure | A detailed disclosure of the data has been impacted (e.g., passwords, financial information) [15]. |
| Customer advice | Recommendations are provided on how customers should move forward after the incident (e.g., changing a password, monitoring credit) [15]. |

Following the qualitative coding, we used an inductive approach to search for patterns in the grouping of characteristics across the entire pool of cybersecurity incident notifications. We sought to identify both "extreme" types of incident notifications (i.e., uncommon, radical strategies), as well as "typical" responses (i.e., commonly adopted strategies). By iteratively reviewing our incident coding results, we began to identify similarities in how some organizations responded. Based on these initial similarities, we constructed a preliminary matrix of notification characteristic groupings. As we continued examining more of the coding results, these groupings were refined. Early in the process, we identified five distinct groups, but this was later extended to eight, and then finally reduced down to six. Collectively, we refer to these as *notification types*. Refer to Table 2 for details, where each type represents a collection of characteristics that were coded as being either present (e.g., the organization apologized in the notification; indicated with a "Y" in Table 3) or absent (e.g., the organization did not apologize; indicated with an "N" in Table 3). Those characteristics that are not explicitly considered as part of a notification type are indicated with a "-". Three of these types (full transparency, guarded, and opacity) are grouped together as they are all concerned with the *level of detail contained within the notice*, while the other three types (customer interest, balanced interest, and company interest) are grouped together due to their orientation around *the party that benefits from the notification strategy*.

Table 2. Incident Notification Types

| Notification Type | Definition |
|---|---|
| Full transparency | A notification is fully forthcoming and contains comprehensive details pertaining to the incident without whitewashing. A clear organizational response is specified, as well as a value commitment. |
| Guarded | A notification discloses minimal information relevant to the incident, while also whitewashing the company's responsibility for the event. However, a clear organizational response is specified, as is a value commitment. |
| Opacity | A notification discloses minimal information relevant to the incident, while also whitewashing the company's responsibility for the event. Although there is responsive action noted, there is no value commitment. |
| Customer interest | A notification contains information that primarily benefits customers. The company takes full accountability for the incident, while also giving customers advice and compensation. |
| Balanced interest | A notification contains information that benefits both the customer and the company. Though customers are not compensated, the company takes full accountability for the incident. |
| Company interest | A notification contains information that primarily benefits the company. The company takes no accountability for the incident, gives no advice to customers, and offers no compensation. |

Table 3. Coding Types

| | Notification Characteristics | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Notification Type | Detailed Explanation | Whitewashing | Apology | Compensation | Responsive Action | Value Commitment | Customer Focus | Open Disclosure | Customer Advice |
| Full Transparency | Y | N | - | - | Y | Y | - | Y | - |
| Guarded | N | Y | - | - | Y | Y | - | N | - |
| Opacity | N | Y | - | - | Y | N | - | N | - |
| Customer interest | - | - | Y | Y | - | - | Y | - | Y |
| Balanced interest | - | - | Y | N | - | - | - | - | - |
| Company interest | - | - | N | N | - | - | N | - | N |

In the following section we provide details on how these six notification types were represented across our 187 cybersecurity incidents.

## 4. Results

The cybersecurity incidents that formed a basis for our study spanned the first six months of 2020, with February (39) and May (40) containing the highest quantity of notifications. Refer to Table 4 for details. In terms of the originating country of the notification, the United States was most common (133), followed by Canada (15) and the United Kingdom (12). As well, notifications were most commonly identified from organizations in the healthcare sector (55), followed by education (25), and retail (24).

Table 4. Organization and Incident Details

| Category | Description |
|---|---|
| Month | January: 29 (15.5%)<br>February: 39 (20.9%)<br>March: 22 (11.8%)<br>April: 24 (12.8%)<br>May: 40 (21.4%)<br>June: 33 (17.6%) |
| Country | United States: 133 (71.1%)<br>Canada: 15 (8.0%)<br>United Kingdom: 12 (6.4%)<br>Australia: 6 (3.2%)<br>Japan: 5 (2.7%)<br>Other: 16 (8.6%) |
| Industry | Healthcare and Medical: 55 (29.4%)<br>Educational Institutions: 25 (13.4%)<br>Retail: 24 (12.8%)<br>Government and Military: 22 (11.8%)<br>Technology: 18 (9.6%)<br>Other: 15 (8.0%)<br>Finance and Insurance: 14 (7.5%)<br>Hospitality: 9 (4.8%)<br>Non-profit: 5 (2.7%) |

In terms of the basic presence or absence of the nine notification characteristics, 72% contained a detailed explanation, 35% included whitewashing elements, 52% contained an apology, 35% included compensation, 94% had responsive action, 83% had a value commitment, 93% articulated a focus on customers, 78% were disclosed openly, and 68% contained advice. Refer to Table 5 for details.

Table 5. Notification Characteristic Coding

| Characteristic | Yes | No |
|---|---|---|
| Detailed explanation | 135 (72%) | 52 (28%) |
| Whitewashing | 65 (35%) | 121 (65%) |

| | | |
|---|---|---|
| Apology | 98 (52%) | 89 (48%) |
| Compensation | 66 (35%) | 121 (65%) |
| Responsive action | 175 (94%) | 12 (6%) |
| Value commitment | 155 (83%) | 31 (17%) |
| Focused on customers | 174 (93%) | 13 (7%) |
| Open information disclosure | 146 (78%) | 41 (22%) |
| Customer advice | 128 (68%) | 59 (32%) |

### 4.1. Incident notification types

As noted above, we identified six notification types from our analysis, within two groups. The first group, which contained the full transparency type, the guarded type, and the opacity type, was focused on the level of detail contained within the notice. For instance, an example of the full transparency type came with Pacific Specialty Insurance Company's notification, which included extensive details on the incident, as well as a clear commitment to customers:

> *"The types of information contained within the potentially impacted emails varied by individual but include: an individual's name, Social Security number, driver's license and/or government issued identification, financial information, payment card information, medical information, and health insurance information. Pacific Specialty is committed to, and takes very seriously, its responsibility to protect all data in its possession. Pacific Specialty is continuously taking steps to enhance data security protections. As part of its incident response, it changed the log-in credentials for all employee email accounts to prevent further unauthorized access…Pacific Specialty established a dedicated assistance line for individuals seeking additional information regarding this incident."*
> - Pacific Specialty Insurance Company [42]

In comparison, an example of a guarded notification type was found with the City of Dawson Creek. In this case, although an organizational response is specified, there are relatively few details provided on the incident and the organization downplays the severity of the event (i.e., whitewashing):

> *"In the early hours of Thursday, January 9th, the City of Dawson Creek discovered that it was the victim of a cyber-attack in which the City's network was illegally accessed and infected with ransomware. The malware was able to encrypt a number of City systems, rendering them temporarily unusable. City of Dawson Creek staff worked quickly to isolate the attack and to activate a comprehensive cyber incident investigation and response. The impacted systems were backed up, and all necessary steps are being taken to restore access to systems and files, and to ensure operations and services return to normal as quickly as possible. There is currently no evidence to suggest that any information was removed from the City's systems or inappropriately accessed, and cyber security experts are working quickly to confirm this."* - City of Dawson Creek [43]

Finally, with the opacity type, we found that organizations were much more restrictive with the information they were willing to share. For example, at Enloe Medical Center, the organization provides few details on the incident and downplays the event's severity. There is also no clear commitment to customer security:

> *"Two weeks following a ransomware incident affecting network infrastructure, Enloe Medical Center is nearing full-functional restoration of its core systems. Upon discovery of the Jan. 2 incident, Enloe's comprehensive emergency protocols were immediately implemented to safeguard patient records…The swift, seasoned response of Enloe's Information Technology personnel resulted in major clinical programs being restored and back online within three days of the incident. Ancillary clinical programs were restored and back online shortly thereafter. At this time, there is no indication or evidence that suggests patient data was accessed, or exfiltrated."* - Enloe Medical Center [44]

The second group of notification types, which contained the customer-interest type, the balanced-interest type, and the company-interest type, are oriented towards the party that benefits from the notification strategy. For example, the customer-interest type aims to cater to the concerns and well-being of customers. An example is at Tandem Diabetes Care, where the organization takes accountability for the incident, provides advice on how customers should proceed, and offers compensation in the form of credit monitoring and identity management:

> *"We recommend that customers review the billing statements they receive from their healthcare providers. If they see services they did not receive, they should contact the provider immediately. For those customers whose Social Security numbers were included in the email accounts, we are offering a complimentary membership of credit monitoring and identity protection services. We take the privacy and confidentiality of our customers' information very seriously and apologize for any inconvenience or concern this incident may cause our customers."*
> - Tandem Diabetes Care [45]

In contrast, the balanced interest type attempts to serve the interests of both customers and the company.

For example, the University of Utah Health notification includes the acknowledgement of responsibility, though no customer compensation is offered:

> *"We recommend patients review the statements they receive from their health care providers. If there are discrepancies or services that you did not receive, please contact the provider immediately. We deeply regret any concern or inconvenience this may cause our patients. We are actively reviewing information protocols, reinforcing information security procedures with our employees and implementing changes where needed to help prevent an incident like this from happening again."* - University of Utah Health [46]

Finally, the company-interest type frames its notifications in a protective, defensive way, which seeks to best serve the organization. For example, the following notification from Transavia does not take any accountability for the event, provides no advice for customers, and offers no compensation:

> *"We continuously monitor our IT landscape to track deviating activities. We have recently found that there has been a case of unwanted access to a Transavia mailbox. After investigation, it appeared that this mailbox contained a file with personal data of a number of passengers who traveled with us…We have reported this to the Dutch Data Protection Authority. Despite the fact that this concerns data from the beginning of 2015 and that it did not contain sensitive data such as address data, credit card information or passport information, we [will] personally inform the passengers involved about this event."* - Transavia [47]

## 4.2. Patterns across incident notification types

Of the incident responses that fully aligned with our six identified notification types, 70 were full transparency, 7 were guarded, 1 was opacity, 35 were customer interest, 10 were company interest, and 59 were balanced interest (some notifications belonged to one "level of detail" type, as well as one "benefitting party" type). We also noted that 55 incident notices did not fully align with any of the incident notification types.

Since the full transparency and customer-interest types share similar objectives in terms of information distribution, we expected incidents belonging to one category to also correspond to the other. We found that this was the case with 15 notifications. Similarly, we expected responses that were guarded to overlap with balanced interest and four notices were found to do so. Finally, we expected notifications that were the opacity type to also be company-interest type, but none were. Interestingly, and contrary to our expectations, we also found that three incidents were coded to both full transparency and company interest, while 27 incidents were coded to full transparency and balanced interest. We also noted that one incident was coded to both guarded and customer interest.

# 5. Discussion

The objective of this study was to identify patterns in the approaches used by organizations when notifying customers about cybersecurity incidents. We qualitatively coded the characteristics of 187 notifications associated with cybersecurity incidents that occurred during the first half of 2020. Our results highlighted six distinct notification types. The first three types were grouped together as pertaining to the level of detail in the notice: full transparency, guarded, and opacity. The second three types were grouped together based on the party that benefits from the notification strategy: customer interest, balanced interest, and company interest.

The characteristics of the notifications in our sample were distinct from those in previous studies. In particular, the notifications were drawn from a total of 18 countries, whereas past research [e.g., 18] tends to focus on firms based in the United States or on a two-country comparison [e.g., 16, 36]. This provides a uniquely global perspective on cybersecurity incidents and the associated notification strategies. For example, Kim and Lee [36] examined 108 notifications in the United States and South Korea. They found the most incidents in the retail sector (25.9%), followed by technology (13.9%) and healthcare (12%). In comparison, our sample had the most incidents originating from healthcare (29.4%), followed by education (13.4%) and retail (12.8%). The variation here might be explained by the different countries that were examined, but it could also be attributed to the period in which the Kim and Lee data was collected (2008–2016). For example, the recent rise in ransomware attacks has made healthcare and educational institutions particularly popular targets [48]. However, despite those differences, our results showed similar rates of compensation (35.3%) and whitewashing (34.8%) relative to Kim and Lee's findings (33.3% and 30.5%, respectively).

Compared to other research, such as Diesterhöft et al. [15], our findings also show that a number of the U.S.-based notification characteristics exist similarly in a global dataset. For example, we found that 93.6% of notifications contained responsive actions, 78.1% utilized open disclosure, and 82.9% articulated a value commitment. This compares to 84.3%, 82.1%, and 80.5%, respectively, in Diesterhöft et al. [15]. However, our results suggested fewer apologies (52.4% versus 73.1%) and less customer advice (68.4% versus 89.5%).

In examining the notification type patterns, we found that although some organizations appear to be focusing primarily on their own interests (1 opacity; 10 company interest), many more organizations are at least partially (7 guarded; 59 balanced interest) or fully committed (70 full transparency; 35 customer interest) to serving customers with informative cybersecurity incident notifications.

## 5.1. Contributions

From a research perspective, the six notification types that emerged from our study extend past work that identify the notification characteristics that are utilized by organizations during cybersecurity incidents. Based on the empirical data we collected, these six types provide unique insights into how these various characteristics are assembled within a notification. Indeed, these types may provide valuable clues into the strategic style that organizations employ when managing crisis situations. This line of inquiry follows past calls [e.g., 15] for research investigating the strategy used to select incident notification approaches. In doing so, our findings complement past work by Wang and Kuo [49], who consider potential links between an organization's crisis response capabilities and its strategic style in terms of the prospector, defender, and analyzer typology proposed by Miles and Snow [50]. Wang and Kuo [49] find that where an organization has established a general strategic direction, its crisis response capabilities will be improved. To the extent that the notification types identified in our findings contain characteristics that are consistent and compatible with one another, it may indicate that the firm has established a broader strategy that has been operationalized within the crisis response activities. Likewise, those firms that simultaneously employ notification characteristics that are seemingly at odds with one another (e.g., whitewashing and compensation) may indicate that an organization has opportunities to establish a guiding strategic style.

Our work also provides a distinctly global view of cybersecurity incident notifications. Since nearly 30% of our incident notifications were drawn from countries other than the United States, our results suggest that international approaches appear similar to the United States in some respects (e.g., value commitment) but are distinct in others (e.g., apologies).

From a practical perspective, our findings point out how common characteristics of cybersecurity incident notifications are assembled. For new organizations or those struggling to decide on a consistent incident notification approach, the notification types highlighted in our findings can provide several possible options that could be considered for adoption. For organizations with a more mature incident notification approach that already corresponds to one of our notification types, our findings may help to highlight additional notification characteristic refinements that could be added in future notifications for improved consistency.

## 5.2. Limitations and future research

As with any research study, our work is subject to limitations that provide promising opportunities for future research. First, we acknowledge that for some cybersecurity incidents, no customer notification was produced (e.g., due to the lack of requirements to do so) and in others, the notification was not available (e.g., the organization removed it from its website). As a result, our findings are derived from those notifications that were publicly accessible at the time of our study. An interesting direction for future research may be to examine the characteristics of organizations that do and do not issue a customer notification following a cybersecurity incident.

Second, although our study draws on 54 incident notifications originating from non-U.S. organizations, our analysis remains weighted towards incidents from U.S. organizations. Future research could extend this international focus by drawing on a wider time period to gain further insights into the patterns of cybersecurity notifications that exist around the world. As we note in our findings, 55 of our collected incident notifications did not fully fit into any of our six notification types. Interestingly, only 9 (16%) of these were from non-U.S. organizations, even though our sample was 29% international. This suggests that our identified notification types may align better with non-U.S. organizations and that future research could seek to find additional notification types used in U.S. organizations.

Third, our study examined notifications associated with individual cybersecurity incidents, but it remains unclear how notification strategies may change within a single organization for successive incidents. A promising opportunity for future research would be to conduct a longitudinal analysis of the extent that an organization uses similar or different incident notification approaches for different cybersecurity breaches that occur over time.

Finally, although our study identifies patterns within the characteristics of cybersecurity incident notifications, we stop short of connecting the resulting notification types to a measure of crisis response effectiveness. Future research could investigate if some notification types tend to correspond with particular downstream consequences such as customer lawsuits or customer retention. Establishing an empirical relationship between an organization’s notification type and measurable customer consequences could further solidify the importance of notification choices as part of an organization’s cybersecurity crisis response.

## 6. Conclusion

This study set out to identify patterns contained within cybersecurity incident notifications by constructing a typology of response approaches. Based on analysis of 187 notifications, we identified three distinct types associated with the notification’s level of detail and three response types associated with the benefitting party. Our findings extend past classifications of cybersecurity incident notifications and provide a template of possible notification approaches to be adopted by organizations.

## 7. References

[1] Ponemon Institute, "Cost of a Data Breach Report", 2020. [Online]. Available: https://www.ibm.com/security/data-breach

[2] Verizon, "2020 Data Breach Investigations Report", Verizon, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/

[3] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide", National Institute of Standards and Technology, 2012, Special Publication 800-61, Revision 2. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

[4] Office of the Privacy Commissioner of Canada, "A Full Year of Mandatory Data Breach Reporting: What We’ve Learned and What Businesses Need to Know", https://priv.gc.ca/en/blog/20191031/ (accessed April 21, 2021).

[5] A. Bitektine and P. Haack, "The ‘Macro’ and the ‘Micro’ of Legitimacy: Toward a Multilevel Theory of the Legitimacy Process", Academy of Management Review, Academy of Management, Briarcliff Manor, NY, 2015, pp. 49-75.

[6] M. M. Zhan and X. Zhao, "How Stakeholders React to Issues with Risk Implications: Extending a Relational Perspective of Issues Management", Journal of Contingencies and Crisis Management, Wiley, New York, NY, 2021, pp. 1-14.

[7] H. Cavusoglu, B. Mishra, and 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, 2004, pp. 69-104.

[8] A. Hovav and J. D'Arcy, "The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms", Risk Management and Insurance Review, Wiley, Hoboken, NJ, 2003, pp. 97-121.

[9] A. A. Yayla and Q. Hu, "The Impact of Information Security Events on the Stock Value of Firms: The Effect of Contingency Factors," Journal of Information Technology, Sage, New York, NY, 2011, pp. 60-77.

[10] R. D. Banker and C. Feng, "The Impact of Information Security Breach Incidents on CIO Turnover," Journal of Information Systems, American Accounting Association, Lakewood Ranch, Fl, 2019, pp. 309-329.

[11] T. J. Smith, J. L. Higgs, and R. Pinsker, "Do Auditors Price Breach Risk in Their Audit Fees?", Journal of Information Systems, American Accounting Association, Lakewood Ranch, FL, 2019, pp. 177-204.

[12] Delaware Attorney General, "Cyber-Incident Customer Notification - Delware Template", https://attorneygeneral.delaware.gov/wp-content/uploads/sites/50/2018/11/Travel-Leaders-Group-Data-Breach-Customer-Notification-Delaware-State-Template.pdf (accessed April 21, 2021).

[13] Educase, "Data Incident Notification Toolkit", https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/data-incident-notification-toolkit (accessed April 21, 2021).

[14] Montana Department of Justice, "Sample Data Breach Notification", https://dojmt.gov/wp-content/uploads/Glasswasherparts.com_.pdf (accessed April 21, 2021).

[15] T. Diesterhöft, K. Masuch, M. Greve, and S. Trang, "Really, What Are They Offering? A Taxonomy of Companies' Actual Response Strategies after a Data Breach", in *15th Pre-ICIS Workshop on Information Security and Privacy*, 2020, pp. 1-17.

[16] M. Greve, K. Masuch, S. Hengstler, and S. Trang, "Overcoming Digital Challenges: A Cross-Cultural Experimental Investigation of Recovering from Data Breaches", in *Forty-First International Conference on Information Systems*, AIS Virtual Conference Series, 2020, pp. 1-17.

[17] M. Greve, K. Masuch, and S. Trang, "The More, the Better? Compensation and Remorse as Data Breach Recovery Actions – An Experimental Scenario-based Investigation", presented at the 15th International Conference on Wirtschaftsinformatik, 2020.

[18] K. Masuch, M. Greve, and S. Trang, "Please be Silent? Examining the Impact of Data Breach Response Strategies on the Stock Value", in *Forty-First International Conference on Information Systems*, AIS Virtual Conference Series, 2020, pp. 1-17.

[19] NIST, "Supplemental Information for the Interagency Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity", 2015. [Online]. Available: http://dx.doi.org/10.6028/NIST.IR.8074v2

[20] M.-D. McLaughlin and J. Gogan, "Challenges and Best Practices in Information Security Management", MIS Quarterly Executive, 2018, pp. 237-262.

[21] T. V. Eaton, J. H. Grenier, and D. Layman, "Accounting and Cybersecurity Risk Management", Current Issues in Auditing, American Accounting Association, Sarasota, FL, 2019, pp. C1-C9.

[22] S. Walton, P. Wheeler, Y. Zhang, and X. Zhao, "An Integrative Review and Analysis of Cybersecurity

Research: Current State and Future Directions", Journal of Information Systems, American Accounting Association, Lakewood Ranch, FL, 2021, pp. 155-186.

[23] T. Wang, K. N. Kannan, and J. R. Ulmer, "The Association Between the Disclosure and the Realization of Information Security Risk Factors", Information Systems Research, INFORMS, Catonsville, MD, 2013, pp. 201-218.

[24] M. Buckbee, "Data Breach Definition by State", Varonis. https://www.varonis.com/blog/data-breach-definition-by-state/ (accessed April 24, 2021).

[25] M. J. Bitner, B. H. Booms, and M. S. Tetreault, "The Service Encounter: Diagnosing Favorable and Unfavorable Incidents", Journal of Marketing, American Marketing Association, 1990, pp. 71-84.

[26] D. P. Millar and R. L. Heath, *Responding to Crisis: A Rhetorical Approach to Crisis Communication*, Lawrence Erlbaum, Mahwah, NJ, 2004.

[27] W. T. Coombs, "The Protective Powers of Crisis Response Strategies", Journal of Promotion Management, Taylor & Francis, Oxfordshire, UK, 2006, pp. 241-260.

[28] S. Marsen, "Navigating Crisis: The Role of Communication in Organizational Crisis", International Journal of Business Communication, Sage Journals, New York, NY, 2020, pp. 163-175.

[29] S. Tucker, N. Turner, J. Barling, E. M. Reid, and C. Elving, "Apologies and Transformational Leadership", Journal of Business Ethics, Springer, New York, NY, 2006, pp. 195-207.

[30] D. P. Skarlicki, R. Folger, and J. Gee, "When Social Accounts Backfire: The Exacerbating Effects of a Polite Message or an Apology on Reactions to an Unfair Outcome", Journal of Applied Social Psychology, Wiley, Hoboken, NJ, 2004, pp. 322-341.

[31] W. T. Coombs and S. J. Holladay, "How Publics React to Crisis Communication Efforts: Comparing Crisis Response Reactions Across Sub-arenas", Journal of Communication Management, Emerald Publishing, Bingley, UK, 2014, pp. 40-57.

[32] J. E. Massey, "Managing Organizational Legitimacy: Communication Strategies for Organizations in Crisis", Journal of Business Communication, Sage Journals, New York, NY, 2001, pp. 153-183.

[33] D. Fischer, O. Posegga, and K. Fischbach, "Communication Barriers in Crisis Management: A Literature Review", in *Twenty-Fourth European Conference on Information Systems*, Istanbul, Turkey, 2016, pp. 1-18.

[34] A. Malhotra and C. K. Malhotra, "Evaluating Customer Information Breaches as Service Failures: An Event Study Approach", Journal of Service Research, Sage Journals, New York, NY, 2011, pp. 44-59.

[35] S. Goode, H. Hoehle, V. Venkatesh, and S. A. Brown, "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony Playstation Network Breach", MIS Quarterly, Minneapolis, MN, 2017, pp. 703-727.

[36] N. Kim and S. Lee, "Cybersecurity Breach and Crisis Response: An Analysis of Organizations' Official Statements in the United States and South Korea", International Journal of Business Communication, Sage Journals, New York, NY, 2018, pp. 1-22.

[37] J. D. Collins, V. A. Sainato, and D. N. Khey, "Organizational Data Breaches 2005-2010: Applying SCP to the Healthcare and Education Sectors", International Journal of Cyber Criminology, K. Jaishankar, Ahmedabad, Gujarat, India, 2011, pp. 794-810.

[38] H. Li, W. G. No, and T. Wang, "SEC's Cybersecurity Disclosure Guidance and Disclosed Cybersecurity Risk Factors", International Journal of Accounting Information Systems, Elsevier, Amsterdam, Netherlands, 2018, pp. 40-55.

[39] V. J. Richardson, R. E. Smith, and M. W. Watson, "Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches", Journal of Information Systems, American Accounting Association, Lakewood Ranch, FL, 2019, pp. 227-265.

[40] IT Governance Limited, "IT Governance UK Blog", https://www.itgovernance.co.uk/blog (accessed April 25, 2021).

[41] R. Fehr and M. J. Gelfand, "When Apologies Work: How Matching Apology Components to Victims' Self-construals Facilitates Forgiveness", Organizational Behavior and Human Decision Processes, Elsvier, Amsterdam, Netherlands, 2010, pp. 37-50.

[42] Pacific Specialty Insurance Company, "Pacific Specialty Insurance Company Provides Notice of Data Security Incident", https://www.prnewswire.com/news-releases/pacific-specialty-insurance-company-provides-notice-of-data-security-incident-301010131.html (accessed April 27, 2021).

[43] City of Dawson Creek, "Notice to the Public January 10th", https://www.dawsoncreek.ca/2020/notice-to-the-public-january-10th/ (accessed April 27, 2021).

[44] Enloe Medical Center, "Enloe's Clinical Programs Fully Restored Following Ransomware Incident", https://www.enloe.org/newsroom/news-stories?news=1141 (accessed April 27, 2021).

[45] Tandem Diabetes Care, "Tandem Diabetes Care Notifies Customers of Phishing Incident", https://www.databreaches.net/tandem-diabetes-care-notifies-customers-of-phishing-incident/ (accessed April 27, 2021).

[46] University of Utah Health, "Unauthorized Data Access Alert", https://healthcare.utah.edu/publicaffairs/news/2020 (accessed April 27, 2021).

[47] Transavia, "Unwanted Access to a Transavia Mailbox", https://www.transavia.com/en-EU/incident/ (accessed April 27, 2021.

[48] IBM, "IBM X-Force Threat Intelligence Report 2021", IBM Security, Somers, NY, 2021. [Online]. Available: https://www.ibm.com/security/data-breach/threat-intelligence

[49] C.-y. Wang and M.-f. Kuo, "Strategic Styles and Organizational Capability in Crisis Response in Local Government", Administration & Society, Sage, New York, NY, 2017, pp. 798-826.

[50] R. E. Miles and C. C. Snow, *Organizational Strategy, Structure, and Process*. McGraw-Hill, New York, NY 1978.