

Conceal or Communicate? Organizational Notifications to Stakeholders Following Ransomware Attacks

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

Jonathan Yuan
University of Waterloo
j95yuan@uwaterloo.ca

Albert Chan
University of Waterloo
ak24chan@uwaterloo.ca

Dennis Joo
University of Waterloo
chanwoo.joo@uwaterloo.ca

Abstract

Ransomware attacks have become an unrelenting frustration for organizations of all sizes, industries, and locations. Although past research has examined how ransomware attacks can be more effectively prevented, little attention has been paid to understanding how organizations communicate with stakeholders. In contrast to some cyber incidents that remain hidden for months, ransomware attacks render systems inoperable immediately, which often requires a unique stakeholder response strategy. Drawing on principles from stakeholder theory and crisis response strategies, we examine the organizational communications following 101 ransomware attacks. Our results indicate that stakeholder notifications tend to be either customer-focused or investor-focused, but are rarely both. We also find that most notifications contain at least a basic level of detail, but that about one in ten communications are insufficiently informative. This work extends the field's understanding of cybersecurity incident notifications within the unique context of ransomware attacks and reveals practical insights for cybersecurity managers.

Keywords: Cybersecurity, ransomware, organizational responses, stakeholders

1. Introduction

Ransomware attacks continue to plague organizations in practically every industry across the world. The consequences of successful attacks are significant, with 90% of organizations experiencing an impact to their operations and 86% experiencing a loss of business, with the average recovery cost for these attacks in the range of \$1.4M (Sophos, 2022). Unsurprisingly, company leaders rate ransomware

attacks among the top business-related concerns (Huq, 2022).

Ransomware attacks date back to 1989 and refer to the application of malicious software by external parties on a company's digital asset, such as a system or data, that demands payment in order to restore access (Oz et al., 2022; Savage et al., 2015). In recent years, ransomware attacks have evolved to also include the theft of information, alongside additional payment demands in exchange for non-disclosure of the stolen data (Barker et al., 2021).

Despite increasing investments to defend against ransomware (The Economist, 2021), estimates indicate that approximately 66% of organizations still fall prey to attacks annually (Sophos, 2022). Although many organizations have implemented strategies and plans that cover a variety of possible cybersecurity incidents, managers still struggle to facilitate effective response activities following ransomware attacks (Indyk, 2020).

Part of the challenge is that no single, authoritative framework exists to guide organizations on how to respond to ransomware attacks (Ransomware Taskforce, 2021). In particular, it can be challenging to decide on who needs to be notified, when the communication should occur, and how much to say (Stevens, 2021). Although stakeholder communications following any cybersecurity incident can be challenging, the lack of a standardized reporting approach for ransomware communications can be burdensome for organizations because of the time sensitivity (e.g., a customer-facing system is suddenly rendered inoperable), the unavailability of typical stakeholder communication mediums (e.g., the email system is unable to be used to contact customers), and the lack of clarity on the situation (e.g., personal data may only be locked or may be both locked and stolen) (Ransomware Taskforce, 2021).

Although researchers and practitioners are paying increasing attention to various infection vectors, malicious actions, and extortion methods (Oz et al., 2022; Sophos, 2022), stakeholder communication activities are often viewed as less critical. However, this conclusion fails to recognize the importance that effective reporting of cybersecurity incidents can have for mutually benefiting the ecosystem of customers, regulators, law enforcement organizations, and cybersecurity service providers. For example, a recent ransomware attack at UMass Memorial Health led to a class action lawsuit (and \$1.2M settlement) by employees claiming that the incident led to incorrect wages and delayed payroll deposits (Campus Safety, 2023). Indeed, a recent report points out that “increasing cyber incident reporting and reciprocal information sharing, including through more proactive government dissemination, will help complete the picture of the ransomware threat, and provide potential pathways to mitigate it” (Ransomware Taskforce, 2023, p. 9).

In order to shed light on this important issue, we posed the following research question: *What patterns are present in the approaches used by organizations when notifying stakeholders about ransomware incidents?* In response, we collected information associated with 101 ransomware attacks and identified the related notifications. We qualitatively analyzed the data using principles from stakeholder theory and crisis response strategies.

Our results indicate that most stakeholder notifications are either customer-focused or investor-focused, but are rarely both. We also find that most notifications contain an appropriate level of detail, but that about a tenth of communications are insufficiently informative. Finally, we find that the channel the firm uses to notify its stakeholders can influence the notification characteristics and type of response. These insights contribute to providing a ransomware-specific lens for interpreting the strategies used for attack responses. We highlight common practices, but also improvement opportunities for organizations struggling to navigate the ransomware notification process.

2. Conceptual background

Ransomware has evolved in the three decades since its emergence, but its aims remain largely unchanged: deny rightful access to a digital asset, such that payment can be demanded in order to restore access (Oz et al., 2022; Savage et al., 2015). Recent forms of ransomware attacks supplement the traditional attack approach alongside the threat of disseminating stolen data if the ransom is not paid.

The average ransom payment in 2022 totaled \$812,360, up 480% from 2020 (Sophos, 2022).

However, the operational impact and revenue loss following a ransomware attack can be even more significant. Sophos (2022) reports that in 90% of attacks, organizations suffered an operational impact and 86% experienced a loss of revenue. On average, remediation costs were estimated at \$1.4M per attack and recovery time took approximately one month.

Even though ransomware may have severe consequences, over a quarter of organizations in 2022 are still unprepared to respond to an attack (Barracuda Networks, 2023). One key response area that is often overlooked concerns communications with organizational stakeholders, such as customers or suppliers, who may be impacted by a systems outage. While the occurrence of a ransomware incident may not legally require a company to file a formal notification, this depends on contextual characteristics such as the location of the incident and the nature of the data impacted. Some organizations may elect to be forthcoming in communicating with stakeholders in order to provide an update or express their regret to customers and investors for any inconvenience caused by the incident (Cram & Mouajou-Kenfack, 2022). In the following section, we provide a summary of the crisis response literature that informs the approach organizations take when seeking to manage a cybersecurity incident.

2.1. Crisis response strategies

Although the crisis response literature has a deep history in fields such as marketing and communication (e.g., Bitner et al., 1990; Coombs, 2006; Coombs & Holladay, 2014; Millar & Heath, 2004), research within the cybersecurity literature tends to center on either risk management activities such as formal recovery plans (e.g., Sahebjamnia et al., 2015) or the technical steps needed to recover hardware and data following an incident (e.g., Hull et al., 2019). Although recent work has begun to evaluate the characteristics of communication strategies employed by organizations in response to cybersecurity incidents generally (e.g., Cram & Mouajou-Kenfack, 2022; Diesterhöft et al., 2020; Greve, Masuch, Hengstler, et al., 2020; Greve, Masuch, & Trang, 2020; Masuch et al., 2019, 2020), we are unaware of any ransomware-specific investigations.

When it comes to practical guidance disseminated to managers in the context of ransomware, communication to stakeholders isn't ignored, but little actionable guidance is actually articulated in terms of particular strategies. For example, in the ransomware playbook published by the Canadian Centre for Cybersecurity (2021), it is suggested that “it is imperative you inform key stakeholders, clients, and your staff members. You should consider preparing a

statement in advance that can then be tailored to the incident, as well as a contact list of all stakeholders to be notified” (p. 28). Although such advice acknowledges that stakeholder communications are indeed important, it falls short of providing insights into the timing, content, and level of detail that should be included. Other guidance points out simple observations, such as that internal email may not be available in the event of a successful ransomware attack (e.g., Hawkins, 2018). However, a key challenge faced by management in responding to ransomware attacks is appropriately notifying those stakeholders whose activities could be impacted by the incident, while not providing so much information that it could lead to costly litigation, embarrassing retractions, or attention that could lead to additional attacks. For example, Morgan and Gordijn (2020) consider the responsibilities of the business alongside the interests of stakeholders, which include shareholders, employees, the local community, customers, suppliers, competitors, and the general public. In order to reconcile these diverse viewpoints, we turned to past work on stakeholder theory, which we describe in the following section.

2.2. Stakeholder theory

Rooted in the strategic management literature, stakeholder theory is oriented toward the premise that company leaders have a duty not only to shareholders (i.e., owners) but also to any individuals or groups with an interest in the firm (Flak & Rose, 2005). Although precisely what level of interest is sufficient to qualify as a stakeholder is the subject of some dispute, a common view is that a stakeholder is “any group or individual who can affect or is affected by the achievement of the organization’s objectives” (Freeman, 1984, p. 46). Broadly, such groups would include investors, customers, employees, governments, suppliers, and community groups. In order to fulfill this duty, stakeholder theory suggests that executives should respect the rights of all stakeholders and adopt company policies/structures that equally consider legitimate stakeholder interests (Donaldson & Preston, 1995; Smith, 2008).

Although stakeholder theory has been applied within a variety of normative, descriptive, and operational contexts, one of its overriding management propositions is that companies have an ethical duty to act in line with stakeholder interests, which can in turn improve company performance and trustworthiness (Flak & Rose, 2005). Indeed, Bridoux and Stoelhorst (2022) suggest that stakeholder theory “explicitly incorporates an economic dimension (value creation), a social dimension (managing relationships) and a moral dimension (fairness)” (p. 798).

Within a cybersecurity context, stakeholder theory is not widely applied, perhaps due to the primarily internally facing, protective mindset of much research in the field. However, in the context of responding to cybersecurity incidents, stakeholder theory can provide a potentially valuable lens with which to interpret the various strategies that are available to managers. In the following section, we outline our research approach, which leverages past work on crisis response strategies and the principles of stakeholder theory to explore the characteristics of organizational communications following 101 ransomware attacks.

3. Methodology

Our study consisted of a qualitative analysis of the stakeholder notifications made by organizations following a successful ransomware attack. We started our data collection by first identifying a list of ransomware incidents within the cybersecurity module of the Audit Analytics research database. We accessed the database in January 2023 and retrieved all reported cybersecurity incidents that were categorized as “ransomware” in the attack type. We obtained 115 ransomware incidents, ranging from 2017 to 2022. For each ransomware incident, the database provides information on the target firm, the ransomware attack (i.e., type of information that was accessed, number of records lost), and a link to supplementary information (e.g., news report, regulatory filing). Focusing on incidents from the past several years allowed us to consider not only the immediate notifications made to stakeholders after an attack but also the follow-up notifications that may have occurred months or even years later.

Next, we conducted an in-depth review of each ransomware incident using publicly available information. We started by conducting a web search for supplementary information related to the attack. Our search included the victim organization’s social media accounts, corporate website, regulatory filings, and third-party sources (e.g., news reports). In particular, we focused on locating any notifications made by the organization to any company stakeholders, including customers, investors, and regulators. We paid careful attention to the timing, content, and medium used for the notification. Contextual information was also recorded, where available, including the date of breach discovery and date of breach disclosure. In total, across the 115 incidents in our sample, we were able to locate at least one stakeholder notification for 101 incidents. We note that one incident was removed from consideration as it had been incorrectly coded as a ransomware incident in the database. For those incidents where no notification was found, it could be that the notification was removed

before our research took place, the notification was not posted online (e.g., it was sent by mail or email), or no notification was made.

3.1. Data analysis

For our analysis, we adopted a qualitative approach to analyze the content of the notifications associated with each ransomware attack. This technique was appropriate because it allowed the authors to thoroughly review each notification to consider the content, context, and language used. The objective of our analysis was to identify patterns that reflect common characteristics across the notifications and our approach permitted us to capture the nuances contained within the texts.

We initially started with nine cybersecurity incident characteristics that were identified in prior, non-ransomware-specific research (Cram & Mouajou-Kenfack, 2022; Diesterhöft et al., 2020; Fehr & Gelfand, 2010; Goode et al., 2017; Masuch et al., 2020). The nine incident characteristics were detailed explanation, whitewashing, apology, compensation, responsive action, value commitment, focused on the customers, open information disclosure, and customer advice. As we read through multiple ransomware notifications, we noted that some adjustments were required to tailor the coding approach to the context of our study. First, due to the ransomware-specific focus, some of the existing notification characteristics (e.g., compensation) are less applicable to ransomware as they are to general cybersecurity incidents such as traditional data breaches. Second, since firms can issue cybersecurity incident notifications through different channels, some mediums may be more relevant for certain stakeholders, leading firms to tailor the content of their notifications for the intended audience. We sought to consider ransomware-specific information that could be disseminated via these different channels.

Determining the appropriate notification characteristics was an iterative process and required the author team to read and reread the compilation of ransomware notifications, as well as discuss newly emerging trends. During the initial phase of analysis, the author team met on at least a weekly basis to discuss preliminary insights and determine if any refinements should be considered to the notification characteristic list. As a result of this process, we decided to remove compensation, open information disclosure, and customer advice, as we felt that these three characteristics are more relevant to cybersecurity incidents that involve data breaches and data theft rather than ransomware. Moreover, we added two notification characteristics called financial impact and operational impact to reflect how some notifications discussed the direct, time-specific consequences of the ransomware

attack. Finally, we reframed the code for “whitewashing” (i.e., blaming others and downplaying the severity of an incident) to “responsibility acceptance” in order to highlight the active acceptance of responsibility, rather than the intentional avoidance responsibility. In the end, the author team decided on eight notification characteristics. Refer to Table 1 for the list of our notification characteristics and their corresponding definitions.

Table 1. Coding Characteristics

Notification Characteristic	Definition
Detailed Explanation	Recognizes that a ransomware attack has occurred, as well as provides details on what happened and when.
Responsibility Acceptance	The target firm accepts the blame and does not divert it to others (e.g., employees, suppliers).
Responsive Action	Describes the actions taken by the firm in response to the ransomware attack.
Apology	Expression of remorse or regret about the incident.
Value Commitment	Explanation of the company's commitment to security and/or transparency.
Customer Acknowledgement	Explicit recognition of the importance of customers to the company.
Financial Impact	Describes the financial impact (e.g., costs incurred to mitigate the situation and future proof the victim firm) and potential costs (e.g., lawsuits, claims).
Operational Impact	Describes the operational impact (i.e., supply chain, day-to-day operations).

For each ransomware incident notification, the author team coded whether each of the characteristics from Table 1 were present or absent using a shared spreadsheet that was accessible to each author. If the targeted firm issued multiple ransomware incident notifications (i.e., regulatory filing and a customer letter), we considered all the notifications on a consolidated basis. During this stage of the coding process, the author team continued to meet on a weekly basis to discuss progress, any coding difficulties, and the emergence of any patterns in the data.

Table 2. Incident Notification Types

Notification Type	Definition
Transparent	A notification contains informative details pertaining to the incident and the firm's responsive action without avoiding responsibility.
Guarded	A notification contains informative details pertaining to the incident and the firm's responsive action. However, the

	notification downplays the potential risks or impact to the firm.
Opacity	A notification does not provide detailed incident information. The notification is either very minimal or highly generic.
Investor-Focus	The notification discloses any disruptions to daily operations and the financial impact of the incident.
Customer-Focus	The notification includes an apology, articulates a commitment to the security of customer data, and acknowledges the impact the ransomware incident may have on the customer.
Hybrid	The notification includes elements of both investor-focus and customer-focus notifications.

As patterns in notification characteristics were identified, the author team began to generate preliminary notification types highlighted by individual coders raising trends they identified to the wider author team. Each type represents a unique combination of present or absent notification characteristics (refer to Table 2). As the author team reviewed more ransomware incident notifications, we would discuss whether the number and nature of the notification types were appropriate and make refinements when necessary. In the end, we reached stability at six notification types (refer to Table 3).

Table 3. Coding Types

Notification Type	Notification Characteristic						
	Detailed Explanation	Responsibility Acceptance	Responsive Action	Apology	Value Commitment	Customer Acknowledgement	Financial Impact
Transparent	Y	Y	Y	-	-	-	-
Guarded	Y	N	Y	-	-	-	-
Opacity	N	N	-	-	-	-	-
Investor -Focus	-	-	-	-	-	-	Y
Customer-Focus	-	-	-	Y	Y	Y	-
Hybrid	-	-	-	Y	Y	Y	Y

Further, we organized the six notification types within two independent groups. The first group is focused on the informativeness and amount of the content in the notification. This group contains three notification types: transparent, guarded, and opacity. The second group is focused on the target stakeholder of

the notification. This group contains three notification types: investor-focused, customer-focused, and hybrid.

4. Results

Our dataset corresponds with ransomware incidents that were primarily disclosed in 2020 (36%) and 2021 (36%), with most incidents occurring at organizations located in the United States (83%). Our incidents primarily come from firms in the manufacturing (47%) and services (20%) sectors. Refer to Table 4 for further details on the organizations contained in our data.

Table 4. Organization and Incident Details

Category	Description
Year of Disclosure	2017: 4 (4%) 2018: 4 (4%) 2019: 9 (9%) 2020: 36 (36%) 2021: 36 (36%) 2022: 12 (12%)
Country	USA: 84 (83%) Canada: 4 (4%) Other: 13 (13%)
Industry	Agriculture, Forestry & Fishing: 1 (1%) Mining & Construction: 7 (7%) Manufacturing: 47 (47%) Transportation & Utilities: 9 (9%) Wholesale & Retail Trade: 6 (6%) Financial Services: 11 (11%) Services: 20 (20%)

The results of our coding (see Table 5) revealed that 78% of the notifications included a detailed explanation, 52% demonstrated responsibility acceptance, 85% described the firm's responsive action, 78% had an apology, 33% included a value commitment statement, 37% acknowledged their customers, 32% described the financial impact, and 66% described the operational impact. In terms of the number of notifications within each notification type, 42 are transparent, 33 are guarded, 12 are opaque, 16 are customer-focused, 15 are investor-focused, and 4 are hybrid. Thirteen notifications did not align with any of our identified notification types.

Table 5. Notification Characteristic Coding

Characteristic	Yes	No
Detailed Explanation	79 (78%)	22 (22%)
Responsibility Acceptance	53 (52%)	48 (48%)
Responsive Action	86 (85%)	15 (15%)
Apology	79 (78%)	22 (22%)
Value Commitment	33 (33%)	68 (67%)
Customer Acknowledgement	37 (37%)	64 (63%)
Financial Impact	32 (32%)	69 (68%)
Operational Impact	64 (66%)	33 (34%)

We conducted further analysis to determine the notification channel used to communicate with stakeholders, based on the coded notification type (see Table 6). We find that guarded, opacity, and investor-focused notification types predominately use regulatory filings. Letters to affected individuals are more common for customer-focused notifications. Moreover, we find that transparent and customer-focused notifications are more likely to use multiple channels to inform their stakeholders whereas guarded, opacity, and investor-focused notifications are more likely to use a single channel.

Table 6. Notification Channels

Notification Channel	Notification Type					
	Transparent	Guarded	Opacity	Investor-Focus	Customer-Focus	Hybrid
Regulatory Filings	34	32	12	15	9	4
Letter	21	5	1	0	16	3
Website/News Wire	14	8	1	4	2	2
Single Channel	17	22	11	11	6	0
Multiple Channel	25	11	1	4	10	4

4.1 Incident notification types

In this section, we provide examples for each of the six notification types, which are split into two groups that represent elements associated with stakeholder theory. The first group focuses on the informativeness and amount of content within a notification provided to stakeholders. This group contains three notification types: transparent, guarded, and opacity. An example of a transparent notification is when HanesBrands issued a letter to the individuals affected by the company's ransomware attack in May 2022. The letter clearly describes the events of the attack, how the company responded, and the acceptance of the firm's responsibility. Below is an excerpt from the letter:

On May 24, 2022, HanesBrands detected a ransomware incident impacting certain internal IT systems. We took prompt action to contain the incident, secure our systems, restore and resecure impacted data, and implement our business continuity plans. We also reported the incident to law enforcement and have been cooperating with their investigation. After working to restore and resecure impacted data, we conducted a review and recently identified that some of your personal information was impacted in the event. The

impacted information varies by individual, and may have included contact information; date of birth; financial account information; government issued identification numbers such as drivers' license numbers, passport information and social security numbers; and other information related to benefits and employment, including certain limited health information provided for employment-related purposes. The safety of your personal information is of the utmost importance to us. We promptly reported the incident to law enforcement and began an investigation to understand the scope and impact. We have also taken a number of steps to even further strengthen the security of our networks. We are continuing to monitor the dark web for any indication of misuse of personal information in connection with this incident, and to date have not identified any such misuse. – HanesBrands (2022)

In comparison, guarded notifications still provide stakeholders with a detailed account of the ransomware attack and the firm's response, but the severity and impact of the attack is increasingly muted, relative to a transparent approach. For example, IPG Photonics Corporation included the following disclosures in its September 21, 2020, 8-K filing regarding the ransomware attack earlier in the month:

On September 14, 2020, IPG Photonics Corporation (the "Company") detected a ransomware attack impacting certain of its operational and information technology systems. Promptly upon its detection of the attack, the Company initiated response protocols, launched an investigation and engaged the services of cybersecurity and forensics professionals. As of the date hereof, the Company has recovered most of its critical operational data and business systems. Although the Company is in the early stages of assessing the incident, based on the information currently known, the Company does not expect the incident to have a material impact on its business, operations or financial condition. – IPG Photonics Corporation (2020)

Finally, opaque notifications are shorter, more generic, and provide limited information to stakeholders. For example, Allscripts Healthcare Solutions Inc. included the following sentences in its 2017 10-K filing in response to a ransomware attack in January 2018: "Recently, we were subject to a ransomware attack that impacted two of our data centers, resulting in outages that left certain of our

solutions offline for our clients.” – Allscripts Healthcare Solutions Inc. (2017).

The second group of notification types is focused on the audience that the notification is targeted towards, which again links to stakeholder theory principles. This group contains three notification types: investor-focused, customer-focused, and hybrid. An investor-focused notification provides details, targeting a single stakeholder group, on the financial and operational consequences of the ransomware attack. For example, the following is an excerpt from ALJ Regional Holdings Inc.’s December 31, 2021, 10-Q in response to a ransomware attack in August 2018:

Although Faneuil quickly and actively managed the Security Event, such event caused disruption to parts of Faneuil’s business, including certain aspects of its provision of call center services. Faneuil carries insurance, including cyber insurance, commensurate with the size and the nature of its operations. Although Faneuil actively communicated with customers and worked to minimize disruption, Faneuil cannot guarantee that customer relationships were not harmed as a result of the Security Event. As a result of the Security Event, Faneuil incurred expenses of approximately \$0.2 million, recorded in selling, general, and administrative expense during the three months ended December 31, 2021. As of December 31, 2021, Faneuil’s insurance recovery receivable was approximately \$1.1 million, included with other current assets on the Consolidated Balance Sheet, for amounts that are considered probable for recovery. – ALJ Regional Holdings (2021)

In comparison, a notification targeted towards customer stakeholders includes an apology, a value commitment, and a customer acknowledgement. For example, Magellan Health Inc. issued a notice of data breach to its customers in response to the ransomware attack in April 2020. The following is an excerpt from their letter:

Magellan was recently the victim of a criminal ransomware attack. We are writing to let you know how this incident may have affected your personal information and, as a precaution, to provide steps you can take to help protect your information. We take the privacy and security of your personal information very seriously and we sincerely regret any concern this incident may cause you. On April 11, 2020, Magellan discovered it was targeted by a ransomware attack. The unauthorized actor gained access to Magellan’s systems after sending a phishing email

on April 6 that impersonated a Magellan client. Once the incident was discovered, Magellan immediately retained a leading cybersecurity forensics firm, Mandiant, to help conduct a thorough investigation of the incident. The investigation revealed that prior to the launch of the ransomware, the unauthorized actor exfiltrated a subset of data from a single Magellan corporate server, which included some of your personal information...The security of your personal information is important to us and we sincerely regret that this incident occurred. – Magellan Health (2020)

Finally, hybrid notifications reflect concerns that are important to both sets of stakeholders: investors and customers. For example, MaxLinear Inc. addressed their ransomware attack in June 2020 through both a customer letter and an SEC filing. The customer letter included an apology, customer acknowledgement, and a statement of value commitment:

We recently informed you of an incident affecting MaxLinear and are sending this letter to provide you with an update regarding your personal information. Please read this letter carefully and contact us with any questions...On May 24, 2020, we discovered a security incident affecting some of our systems. We immediately took all systems offline, retained third-party cybersecurity experts to aid in our investigation, contacted law enforcement, and worked to safely restore systems in a manner that protected the security of information on our systems...We deeply regret that this incident happened and any concern that this situation has caused. This notification was not delayed due to a law enforcement investigation. We take this situation seriously and have taken and continue to take steps designed to prevent this type of incident from happening in the future. – MaxLinear Inc. (2020a)

Supplementing the customer letter was MaxLinear’s SEC filing, which provided insights into both the financial and operational impact:

On June 16, 2020 MaxLinear, Inc. announced a security incident resulting from a Maze ransomware attack affecting certain but not all operational systems within our information technology infrastructure. The ransomware attack has not materially affected our production and shipment capabilities, and order fulfillment has continued without material interruption...Although we have incurred and will

incur incremental costs as a result of forensic investigation and remediation, we do not currently expect that the incident will materially or adversely affect our operating expenses – MaxLinear Inc. (2020b)

5. Discussion

Our results provide insights about stakeholder notifications following ransomware attacks that extend the current cybersecurity crisis response literature. First, we find that in keeping with the homogeneity of attacked organizations and the lack of a standardized guide for responding to ransomware attacks, organizational notifications are highly varied. Prior research finds that notifications associated with general cybersecurity incidents have distinguishable characteristics that reflect the firm's crisis response strategy (Cram & Mouajou-Kenfack, 2022; Diesterhöft et al., 2020) and we extend this inference to ransomware incidents. In particular, we find that stakeholder notifications reveal patterns that can be categorized based on the amount and informativeness of content that is provided in the notification (i.e., transparent, guarded, opacity) and the identity of the targeted stakeholder of the notification (i.e., investor-focused, customer-focused, hybrid). Our findings extend Cram and Mouajou-Kenfack's (2022) study by also examining the notification characteristics of investor-focused notifications. Investors may not be directly affected by a ransomware attack, but they still bear the consequences through their equity ownership. We find that targeted firms can provide relevant information to investors by discussing how the ransomware attack interrupted daily operations and whether there is a significant financial impact that may affect firm valuation.

Second, our results suggest that the channel used by organizations to notify stakeholders (e.g., regulatory filings, letters to affected individuals, news wires) is closely connected with the notification characteristics and notification types. Consistent with Morgan and Gordijn (2020), this suggests that many organizations undertake some level of prioritization to evaluate the importance of the various stakeholders impacted by a ransomware event and generate notifications to inform these stakeholders. However, though our analysis reveals attention being paid to investors and customers, it remains unclear if organizations do not view other stakeholders such as suppliers and employees as sufficiently important to notify or if they believe that these stakeholders are adequately informed through the existing notifications.

Stakeholder theory suggests that companies should have policies in place to attend to the interests of all

legitimate parties with an interest in the company. Indeed, "stakeholder management requires, as its key attribute, simultaneous attention to the legitimate interests of all appropriate stakeholders, both in the establishment of organizational structures and general policies and in case-by-case decision making" (Donaldson & Preston, 1995, p. 67). As such, companies that attend only to investors or customers, without consideration of those other stakeholders who may be impacted, may be seen as not fulfilling their duty. This is a key aspect of ransomware response that has the potential to be mismanaged organizations when faced with time-sensitive and operationally critical attacks. Further, stakeholder theory suggests that stakeholder roles and perspective may change over time (Pouloudi & Whitley, 1997), suggesting that the policies put in place to facilitate crisis communications should be regularly reviewed for such adjustments.

One interpretation of our findings would suggest that companies should ensure a clear process is in place to communicate with all relevant stakeholders during and after a ransomware attack in a way that those stakeholders find appropriately transparent and informative. This could entail establishing a list of the company's systems and of stakeholders who would be impacted by a ransomware attack. The list may aid management in rapidly identifying the stakeholder groups who should receive incident communications. For example, if an internal system that facilitates the manufacturing process was attacked, then perhaps suppliers and customers would be the primary recipients of incident communications. Alternatively, if a sales system that stored credit card information was successfully attacked, then the stakeholder focus may be oriented toward customers, government officials (i.e., law enforcement, regulators), and financial institutions. Having a degree of dynamism may be critical during incident response activities and, by arranging a semi-structured guide in advance, managers may be more readily able to contact the stakeholders who have the most to gain or lose from the attack.

Although stakeholder theory makes a case for the fair treatment of stakeholders from an ethical standpoint, other research suggests that value creation and competitive advantage can also be realized (Bridoux & Stoelhorst, 2022). From this perspective, those organizations that are more effective in meeting stakeholder expectations in times of crisis may be laying the foundation for long-term growth, rather than merely trying to navigate a short-term speedbump.

5.1. Contributions

The objective of this study was to identify patterns that are present in the approaches used by organizations

when notifying stakeholders about ransomware incidents. In doing so, we extend the field's understanding of cybersecurity incident notifications within the unique context of ransomware attacks by highlighting that stakeholder notifications tend to be either customer-focused or investor-focused, but are rarely both. We also find that most notifications contain at least a basic level of detail, but that about 10% are insufficiently informative. This is of particular importance due to the continued challenge that ransomware attacks pose to today's organizations, alongside the lack of a standardized approach in place to guide ransomware response activities. By drawing on principles of crisis response, alongside stakeholder theory, we also reveal practical insights for cybersecurity managers in terms of the importance of proactively identifying what stakeholders should be communicated with in the event of a ransomware attack, what system outages would necessitate such communication, what details will be provided, and what communication channel will be used.

5.2. Limitations and future research

As with any research project, our study includes limitations that provide future research opportunities. First, observations in our sample are based on publicly available information associated primarily with U.S. firms. Future research could extend our study by obtaining a more global sample of notifications to see if the patterns we identified remain similar globally. Further, alternative data sources could be drawn upon, such as stakeholder interviews. Second, we acknowledge that our dataset represents only a small sample of the ransomware attacks that have taken place over the past several years. Future research could apply our analysis approach to a larger sample to determine if additional patterns emerge. Third, although our study identifies six different notification types, we stop short of investigating the antecedents or consequences of these strategies. Future research could investigate the market, industry, or political circumstances that might lead an organization to employ a particular notification type instead of another. Additionally, it could be valuable to investigate the implications of ransomware notification strategies on indicators associated with stakeholder groups (e.g., stock price, customer turnover, regulatory fines).

6. Conclusion

Our study extends the study of cybersecurity incident notifications to the unique context of ransomware attacks. We adopted a qualitative approach to examine the content of 101 ransomware incident

notifications with the aim of revealing underlying patterns. Our results determine that ransomware notifications can be distinguished by the amount of informativeness of content they provide (i.e., transparent, guarded, and opaque) and the audience that the notification is intended for (i.e., investor-focused, customer-focused, and hybrid). Increased clarity on how organizations navigate this area of ongoing difficulty can help to guide future studies on the key drivers and consequences, as well as aid organizations in more effectively responding to attacks.

7. References

- ALJ Regional Holdings. (2021). Securities and exchange commission form 10-Q. https://www.sec.gov/ix?doc=/Archives/edgar/data/0001438731/000156459022004796/alji-10q_20211231.htm
- Allscripts Healthcare Solutions. (2017). Securities and exchange commission form 10-K. https://www.sec.gov/Archives/edgar/data/1124804/000156459018003105/mdrx-10k_20171231.htm
- Barker, W. C., Scarfone, K., Fisher, W., & Souppaya, M. (2021). Cybersecurity framework profile for ransomware risk management. N. I. o. S. a. Technology.
- Barracuda Networks. (2023). Market report: 2023 ransomware insights. <https://www.barracuda.com/reports/ransomware-insights-report-2023>
- Bitner, M. J., Booms, B. H., & Tetreault, M. S. (1990). The service encounter: Diagnosing favorable and unfavorable incidents. *Journal of Marketing*, 54, 71-84.
- Bridoux, F., & Stoelhorst, J. W. (2022). Stakeholder theory, strategy, and organization: Past, present, and future. *Strategic Organization*, 20(4), 797-809.
- Campus Safety. (2023). UMass memorial to pay \$1.2m to settle wage claims after ransomware attack. <https://www.campussafetymagazine.com/hospital/umass-memorial-to-settle-wage-claims-ransomware-attack/>
- Canadian Centre for Cybersecurity. (2021). Ransomware playbook. <https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099>
- Coombs, W. T. (2006). The protective powers of crisis response strategies. *Journal of Promotion Management*, 12(3-4), 241-260.
- Coombs, W. T., & Holladay, S. J. (2014). How publics react to crisis communication efforts: Comparing crisis response reactions across sub-arenas. *Journal of Communication Management*, 18(1), 40-57.
- Cram, W. A., & Mouajou-Kenfack, R. (2022). Show-and-tell or hide-and-see? Examining organizational cybersecurity incident notifications. *Organizational Cybersecurity Journal*, Advance online publication.
- Diesterhöft, T., Masuch, K., Greve, M., & Trang, S. (2020). Really, what are they offering? A taxonomy of companies' actual response strategies after a data breach. *WIPS 2020*,

- Donaldson, T., & Preston, L. E. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. *Academy of Management Review*, 20(1), 65-91.
- Fehr, R., & Gelfand, M. J. (2010). When apologies work: How matching apology components to victims' self-construals facilitates forgiveness. *Organizational Behavior and Human Decision Processes*, 113, 37-50.
- Flak, L. S., & Rose, J. (2005). Stakeholder governance: Adapting stakeholder theory to e-government. *Communications of the Association for Information Systems*, 16(31), 642-664.
- Freeman, R. E. (1984). *Strategic management: A stakeholder approach*. Pitman.
- Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the sony playstation network breach. *MIS Quarterly*, 41(3), 703-727.
- Greve, M., Masuch, K., Hengstler, S., & Trang, S. (2020). Overcoming digital challenges: A cross-cultural experimental investigation of recovering from data breaches. *Forty-First International Conference on Information Systems, AIS Virtual Conference Series*.
- Greve, M., Masuch, K., & Trang, S. (2020). The more, the better? Compensation and remorse as data breach recovery actions – an experimental scenario-based investigation 15th International Conference on Wirtschaftsinformatik, Potsdam, Germany.
- HanesBrands. (2022). Notice of security incident. <https://www.mass.gov/doc/assigned-data-breach-number-28084-hanesbrands-inc/download>
- Hawkins, N. (2018). Resistance, response and recovery. *Computer Fraud & Security*, 2(-), 10-13.
- Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: Views from a predictive model and human responses. *Crime Science*, 8(2), 1-22.
- Huq, S. (2022). Ransomware: The number one cyber threat for enterprises and SMEs. <https://webarchive.nationalarchives.gov.uk/ukgwa/20221027141254/https://www.ncsc.gov.uk/pdfs/blog-post/ransomware-the-number-one-cyber-threat-for-enterprises-and-smes.pdf>
- Indyk, A. (2020). Stakeholder communications during a ransomware attack. Edelman. <https://www.edelman.ca/insights/stakeholder-communications-during-ransomware-attack>
- IPG Photonics Corporation. (2020). Securities and exchange commission form 8-K. <https://www.sec.gov/Archives/edgar/data/1111928/000111192820000164/ipgp-20200921.htm>
- Magellan Health. (2020). Ransomware attack notice. <https://s3.documentcloud.org/documents/6889299/Magellan-Sample-Individual-Notice.pdf>
- Masuch, K., Greve, M., & Trang, S. (2019). Does it meet my expectations? Compensation and remorse as data breach recovery actions – an experimental scenario based investigation. 14th Pre-ICIS Workshop on Information Security and Privacy,
- Masuch, K., Greve, M., & Trang, S. (2020). Please be silent? Examining the impact of data breach response strategies on the stock value. *Forty-First International Conference on Information Systems, AIS Virtual Conference Series*.
- MaxLinear Inc. (2020a). Notice of data breach. https://oag.ca.gov/system/files/Consumer_Letter%20%2820200610%29.pdf
- MaxLinear Inc. (2020b). Securities and exchange commission form 8-K. <https://www.sec.gov/ix?doc=/Archives/edgar/data/1288469/000128846920000139/mxl-20200616.htm>
- Millar, D. P., & Heath, R. L. (2004). *Responding to crisis: A rhetorical approach to crisis communication*. Lawrence Erlbaum.
- Morgan, G., & Gordijn, B. (2020). A care-based stakeholder approach to ethics of cybersecurity in business. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The ethics of cybersecurity* (pp. 119-138). Springer.
- Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys*, 54(11), 1-37.
- Pouloudi, A., & Whitley, E. A. (1997). Stakeholder identification in inter-organizational systems: Gaining insights for drug use management systems. *European Journal of Information Systems*, 6(1), 1-14.
- Ransomware Taskforce. (2021). *Combating ransomware*. <https://securityandtechnology.org/ransomwaretaskforce/>
- Ransomware Taskforce. (2023). May 2023 progress report. <https://securityandtechnology.org/virtual-library/reports/ransomware-task-force-gaining-ground-may-2023-progress-report/>
- Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, 242(1), 261-273.
- Savage, K., Coogan, P., & Lau, H. (2015). Security response: The evolution of ransomware. Symantec.
- Smith, H. J. (2008). "But what IS the 'right thing'?: Ethics and information systems in the corporate domain. *MIS Quarterly Executive*, 3(2), 105-115.
- Sophos. (2022). The state of ransomware 2022. <https://www.sophos.com/en-us/content/state-of-ransomware>
- Stevens, L. (2021). The rise of ransomware: What communication executives need to know. *Forbes*. <https://www.forbes.com/sites/forbescommunicationscouncil/2021/09/08/the-rise-of-ransomware-what-communication-executives-need-to-know/?sh=348c6cd81a5b>
- The Economist. (2021). Ransomware highlights the challenges and subtleties of cybersecurity. <https://www.economist.com/briefing/2021/06/19/ransomware-highlights-the-challenges-and-subtleties-of-cybersecurity>