On the Importance of Agility, Transparency, and Positive Reinforcement in Cyber Incident Crisis Communication

Tomomi Aoyama, Atsushi Sato, Giuseppe Lisi, and Kenji Watanabe

Nagoya Institute of Technology, Gokiso-cho 4668555, Aichi, Japan
aoyama.tomomi@nitech.ac.jp

Abstract. Cyber incident crisis management protocols often overlook the importance of crisis communication. This paper reviews the crisis communication literature to define explicit communication strategies for each stage of a cyber incident. We applied the proposed model to analyze the Norsk Hydro case: a Norwegian aluminum and renewable energy company halted operations due to a ransomware attack. By combining traditional communication outlets and social media, the company kept high transparency of their recovery operation, with frequent (i.e., agile) updates about the cyber incident. The positive presence of Norsk Hydro on social media allowed them to manage reputation throughout the process. Employees' creativity and loyalty were crucial in the recovery process, and it was promptly publicized globally. This empowered other employees at other branches to act creatively and inspired the community. We conclude the study by suggesting the agility, transparency, and positive reinforcement were the success factor of this crisis communication operation.

Keywords: Cyber incident response · Crisis communication · Information sharing · Communication agility · Transparency · Positive Reinforcement.

1 Introduction

Cyber-attacks continue to pose risks to critical infrastructure. Due to the increasing connectivity, digital and non-digital assets are both vulnerable to threats via Information Communication Technologies [16]. Unlike natural hazards, a cyber incident is caused by the malicious intent of an attacker. Attackers can take advantage of the responding organization's visibility and counteract to the defense.

An example is the Protonmail DDoS (Distributed denial-of-service) attack in 2018 [11]. The initial DDoS attack for the End-to-end encrypted email service provider ProtonMail caused service outage of several minutes. The small hacker group Apophis Squad targeted ProtonMail at random while testing a beta version of a DDoS booter service. Although it was not their intention to persistently attack ProtonMail, but decided to conduct a more massive attack after ProtonMail's CTO, Bart Butler, responded to one of their tweets addressing the group

provocatively[3]. Especially during the cyber incident, the communicator should be aware of the risk of provocation, which leads them to be cautious and be hesitant to communicate to the public.

This study aims at understanding the advantage of active crisis communication operation to the public during a cyber incident. Although the theoretical work on modern crisis communication is extensive, it lacks in reflecting the challenges and benefit from the empirical case studies, particularly in the field of cyber crisis management. We addressed this problem by developing the cyber crisis communication strategy model from the literature review highlighting the shortcomings. Then, we conducted an empirical study of a Norwegian aluminum company's case to analyze the benefit of employing a coordinated communication operation.

2 Cyber Incident Crisis Communication Strategy Model

Crisis communication during the cyber incident should be concurrent with incident response activities. Fig. 1 shows the crisis communication strategy model based on the literature review. In the field of crisis management study, Coombs grouped the crisis communication stages to pre-crisis, crisis-event, and post-crisis [4] as the macro-level framework. Kulikova et al. studied the challenges organization face in cyber incident information disclosure [10]. Steelman [12], Coombs [4], Weiner [17] worked on the best practices of crisis communication.

The research work of Veil [15]is dedicated to determining the advantage and disadvantage of social media use during the crisis. Their findings are incorporated into the Fig. 1, as the cyber incident crisis management activities.

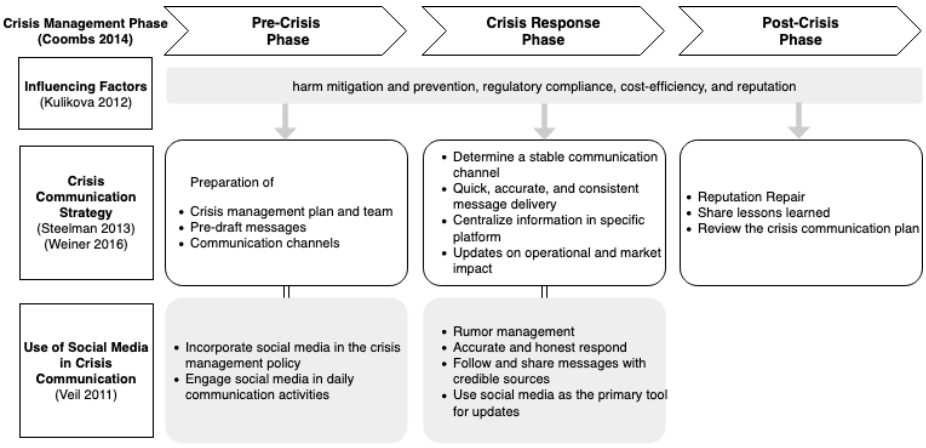

Fig. 1. Cyber incident crisis communication strategy and best practices of social media use in three phases.

From the literature review, we found that previous literature is missing case studies specifically to understand the benefit of utilizing social media in the cyber incident crisis communication. Here, we review a recent cyber incident case and the victim organization's use of social media from the crisis communication perspective.

3 Case Study: Norsk Hydro

The company underwent the production stoppage due to a ransomware attack on the 19th of March 2019. In the following paragraphs, we reconstruct the incident timeline as described on media outlets and the official update by Norsk Hydro (top panel of Fig. 2). As of April 30th 2019, the overall impact on the first quarter of 2019 is NOK 400-450 million (Euro: 45 million; US Dollars: 51 million)[2].

In this section, we describe the crisis communication timeline reconstructed from the social media channels of Norsk Hydro (bottom panel of Fig. 2). On March 19th, the official website of the Norsk Hydro becomes inaccessible. Immediately, the company reports the incident through Twitter and Facebook and establishes the latter as the main channel of communication (i.e., 'Updates regarding the situation will be posted on Facebook'). In the following 24 hours, the Twitter and Facebook accounts of Norsk Hydro posted 7 and 6 updates about the incident, respectively. On March 20th, the company organizes the first press release and Q&A, open to the public via the webcast service `webtv.hegnar.no`, to provide updates about the cyber incident, and publicizes the event via Twitter and Facebook. On March 21st, the official website is recovered, and a new webpage is explicitly created to report about the cyber-incident, and provide the contacts of the public relations personnel.

In the first two weeks after the incident, the company kept a transparent behavior, providing updates on the website and social media (post count on Twitter: 13, Facebook: 8) regarding the operation status. At this stage, the company used the re-tweet function of Twitter to acknowledge the good behavior and creativity of the employees. In early April, the count of social media posts totaled 11 for Twitter and 3 for Facebook. The first Youtube video [8] highlighting the operational personnel's effort was released on April 2nd. On April 9th, the company releases on the official website an article titled 'Employees find creative solutions in response to cyber-attack' [1], and publicizes it on social media. In late April, the count of social media posts decreased to 7 for Twitter and 3 for Facebook, and a second Youtube video [9] was released on April 16th. Finally, on April 30th a preliminary report [2] is published on the official website, while the official report for Q1 2019 is delayed to June 5th, due to the cyber attack impacting the availability of several systems and data. Consistently with the transparent behavior of the company, the report contains the estimated financial and operational loss.

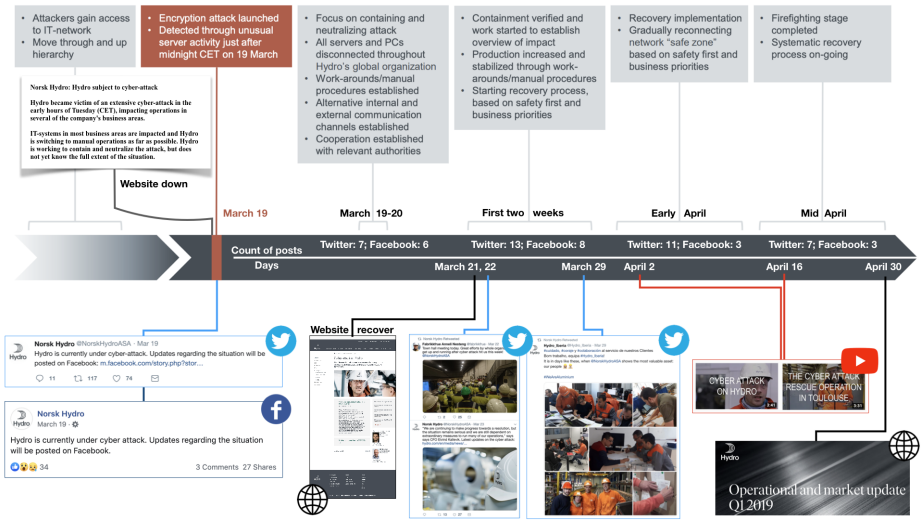

Fig. 2. Timeline of the Norsk Hydro incident [2] (top panel, modified by the author) and the reconstructed highlights of the organizations crisis communication (bottom panel).

4 Lessons Learned

The Norsk hydro case highlighted the benefit of incorporating social media as the medium of crisis communication. During the incident response, the organization continued to show its agility, transparency, and acts of positive reinforcement.

Agility. When the website became unreachable, the organization was quick to determine the alternative platform for communication (facebook and twitter). During the event, multiple platforms were used, including social media and web services. The organization seemed to have a good understanding of each platform; the audience, type of interactions, and its shortcomings. The responding organization has to incorporate the agile process management during the demanding cyber incident response. Agile organizations allow the sharing of information on different levels and between different disciplines, which increases situational awareness and effectiveness [14].

Transparency. Periodic updates on operational status and short documentary videos featuring operators showed honesty and openness. Cornelissen defined transparency as "the state where the image or reputation of an organization held by stakeholder groups is similar to the actual and projected identity of an organization [5]". Transparency creates, maintains, or repairing trust between the organization and stakeholders.

Positive Reinforcement. In the area of psychology and organizational behavior, numerous research has addressed ways to enhance motivation by creating success-focused environments. Interestingly, Norsk Hydro used social media to communicate with the employees. The organization acknowledged the contributions of the employees by retweeting them and created articles and videos highlighting the operators and responders as heroes. Sveen et al. have studied this mechanism in the security incident reporting system in an organization. The result indicates that the increased number of reporting indicates high information security awareness among the system users, and the increase in user motivation causes an increase in the reporting rate, and vice versa [13].

5 Conclusion

In this paper, we studied the Norsk Hydro case from the perspective of crisis communication. From our analysis, we find that risk communication is not only about apologizing or meeting a reporting duty. Instead, it is crucial to promote good behavior of employees by acknowledging their effort. Moreover, by keeping a transparent communication, lessons learned during the recovery operations can be shared with the community.

In the past, information regarding cyber security incidents was shared internally or with close allies. It is because protecting private information is commonly considered as a critical aspect of cyber incident management. Here, we advocate that companies should be more open about sharing information. Haas et al. [7] suggest that Information Sharing and Analysis Organization (ISAO)s create an atmosphere of transparency and inclusion while emphasizing that information sharing, similar to social networking activity, is a group activity and requires active and frequent involvement. In the Norsk Hydro case, in the two weeks following the incident, the company provided updates about the cyber incident with a frequency of at least one post per day, either on Twitter or Facebook.

Undoubtedly, it is still a challenge to ensure the right balance of disclosing and protecting information to defeat an immediate attack and to prepare for long-term security [6]. For this reason, companies should design protocols about what can be shared and what cannot.

The Norsk Hydro demonstrated that agility, transparency, and positive reinforcement are essential principles to promote the good behavior of employees, facilitate cooperation with the relevant authorities and managing reputation.

References

1. Employees find creative solutions in response to cyber-attack (Apr 2019), https://www.hydro.com/en-NO/about-hydro/stories-by-hydro/employees-find-creative-solutions-in-response-to-cyber-attack/
2. Operational and market update q12019 (Apr 2019), https://www.hydro.com/Document/Index?name=Hydro%20Q1-2019%20Update&id=42133

3. Cimpanu, C.: Protonmail ddos attacks are a case study of what happens when you mock attackers (Jun 2018), https://www.bleepingcomputer.com/news/security/protonmail-ddos-attacks-are-a-case-study-of-what-happens-when-you-mock-attackers/
4. Coombs, W.T.: Ongoing crisis communication: Planning, managing, and responding. Sage Publications (2014)
5. Cornelissen, J.P.: Corporate communication. The International Encyclopedia of Communication (2008)
6. Goodwin, C., Nicholas, J.P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., Massagli, A., Mckay, A., Mckitrick, P., Neutze, J., et al.: A framework for cybersecurity information sharing and risk reduction. Microsoft (2015)
7. Haass, J.C., Ahn, G.J., Grimmelmann, F.: Actra: A case study for threat information sharing. In: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security. pp. 23–26. ACM (2015)
8. Hydro, N.: Cyber attack on hydro magnor (Apr 2019), https://www.youtube.com/watch?v=S-ZlVuM0we0
9. Hydro, N.: The cyber attack rescue operation in hydro toulouse (Apr 2019), https://www.youtube.com/watch?v=o6eEN0mUakM
10. Kulikova, O., Heil, R., van den Berg, J., Pieters, W.: Cyber crisis management: A decision-support framework for disclosing security incident information. In: 2012 International conference on cyber security. pp. 103–112. IEEE (2012)
11. ProtonMail: A brief update regarding ongoing ddos incidents (Jul 2018), https://protonmail.com/blog/a-brief-update-regarding-ongoing-ddos-incidents/
12. Steelman, T.A., McCaffrey, S.: Best practices in risk and crisis communication: Implications for natural hazards management. Natural hazards **65**(1), 683–705 (2013)
13. Sveen, F.O., Sarriegi, J.M., Gonzalez, J.J.: The role of incident reporting in reducing information security risk. In: Twenty Seventh International Conference of the System Dynamics Society. The System Dynamics Society (2009)
14. Van Veelen, B., Storms, P., van Aart, C.: Effective and efficient coordination strategies for agile crisis response organizations. Proceedings of ISCRAM 2006 (2006)
15. Veil, S.R., Buehner, T., Palenchar, M.J.: A work-in-process literature review: Incorporating social media in risk and crisis communication. Journal of contingencies and crisis management **19**(2), 110–122 (2011)
16. Von Solms, R., Van Niekerk, J.: From information security to cyber security. computers & security **38**, 97–102 (2013)
17. Weiner, D.: Crisis communications: Managing corporate reputation in the court of public opinion. Ivey business journal **70**(4), 1–6 (2006)