Reserve Bank Information Technology Pvt Ltd

Playbook on Cyber Crisis Communications

Cybersecurity Maturity Model

Abstract:

Cyber Crisis Communication is an important part of the Cyber Crisis Management Plan. Poor handling of an incident can lead to regulatory fines, loss of reputation, and customer trust, and can cause severe damage to company's financials. This playbook describes the crisis communication mechanism organizations may use during a cyber-incident.

Authors

This document is authored by the Research and Innovation team of ReBIT. Shikha Pathak, Research Analyst and Ranjeet Rane, Policy Research Lead worked under the guidance of Vivek Srivastav, former head of the Research and Innovation team. Mr Deepak Maheshwari, an experienced regulatory affairs and communications professional, provided his expert inputs.

Disclaimer: *The mechanisms suggested in the playbook are indicative and not intended to be either exhaustive or mandatory. There may be alternative ways to achieve the same objectives. Organizations may consult experts and implement a strategy most suited and aligned with their own organizational objectives.*

Contents

1. Introduction

1.1 Background

The age old idiom of digging the well when the house catches fire doesn't hold true in the era of internet and social media boom. The traditional approach that involved outright denial, shifting the blame and "allowing the crisis to fade gradually" brings no relief in our increasingly connected digital era. Crises escalate within hours, at unprecedented rates, tarnishing years of goodwill and organizations' reputation. Poor handling of an incident can lead to loss of credibility and customer trust, regulatory fines and can cause severe damage to companies' financials. Effective crisis communication is an important part of the Cyber Crisis Management Plan (CCMP).

1.2 Crisis Communication: Goals and Purpose

The purpose of this paper is to establish guidelines and a put a structural framework in place to help organizations communicate as they prepare for, respond to, mitigate and recover from cyber-incidents. The paper will also suggest strategies to minimize and manage the loss due to delayed or inefficient communication. This can snowball into loss of data and reputation for any organization.

This paper will assist organizations in preparing a crisis communication action plan beforehand as a regulatory and governance foresight. Such manual must clearly define responsibilities and roles to expedite organizations' response time and alleviates chaos and panic during a crisis. To ensure that the organizations adhere to governing mandates including reporting the incident to CERT-IN and other regulatory bodies. For effective and efficient crisis communications, organizations have to invest in people, process and intelligence (in the any order as per the needs of the case), to be able to coordinate and manage in case of a cyber-incident.

Organizations need to map the roles and responsibilities of team members, designate the communication team and select the most relevant channel for the target audience. This ensures that the right message is

shared with the right audience at suitable time. The following infographic exemplifies the various stages an organization goes through to ensure effective communication in case of a crisis:

Preparedness	Identifying Communication Team	Selecting Communication Channels	Message for Target Audience
· CCMP: Incident Management Plan · Maintaining a RACI* Matrix or a linear responsibility chart · Setting up War room · Cyber Crisis Table Top Exercises · RACI: Responsible, Accountable, Consulted, and Informed	· Chief Marketing Officer · Communication Lead · Advisors · Subject Matter Experts · Company Secretary	· Internal and External emails · Press Release to Media · Boardroom Presentation · Regulatory Reporting · Shareholder's Meeting · IVR Service · Notice / Briefing to and via regional office / branch network · Website · Social Media · Customer Support	· Regulator · Board of Directors · Workforce · Third Party · Customers · Insurer · Law Enforcement Agency · Channel Partners · Creditors · Shareholders

Further, for any crisis communication plan, following messaging and communication characteristics may be identified:

- Source of the event
- Goal of the message
- Message content
- Delivery method and channel
- Communicator
- Delivery frequency
- Length and format
- Stakeholder and target audience
- Escalation matrix
- Rights and Obligations of the senders and recipients.

2. Preparedness

A proactive and informed leadership plays a quintessential role in ensuring preparedness for a cyber-event and its aftermath. Pre-crisis communication will need a three pronged approach. There should be mock drills just like fire drills to ensure that the relevant stakeholders are aware of what and how to deal with it in practice rather than the CCMP being consigned to a filing cabinet.

2.1 Advance Scenario Planning

This would begin with identifying internal and external communication risks and preparing of a draft communication plan basis these identified risks. The organization would need to work out a communication flow, this can either be proactive or reactive. This is best decided on a case by case basis as identified in the scenario planning exercise.

2.2 Educate Internal Stakeholders

Internal stakeholders are the first and most important point for communication in the event of a crisis. It is imperative that they are trained and made aware of their roles and responsibilities in the event of a crisis. The correct expectations need to be set with these stakeholders and followed up with a crisis protocol. They should be informed on the steps to initiate as soon as such protocols are executed. Mock drills are one of the recommended activities to be conducted at organization level to ensure optimum levels of preparation and awareness among internal stakeholders.

Well-informed employees are critical to deal with the queries but would often need FAQs. All the same, they must also act with restraint rather than falling for or fueling unofficial or fake news.

2.3 Investing in media relations and external communications

Having a certain degree of control over the message that goes out from the organization goes a long way in safeguarding reputation and public image. Traditional media platforms, particularly print media act as an important medium in putting the message through in the event of a crisis. At the same time, dynamic and interactive platforms like social media also need to be suitably used. Across platforms, the first step would be to identify relevant connections/influencers who can be leveraged in the event of a crisis.

An organization would need to be proactive in sharing information with such stakeholders so that the correct message reaches out to the target audience or the general public, as the case may be. Contrary to traditional practices, it would be in
the benefit of the organization to be more forthcoming in the event of a crisis. Information shared in a transparent manner helps curtail rumors or fake news that may create unnecessary Fear, Uncertainty and Doubt (FUD). Entities must proactively protect their online properties such as official domain names and Twitter handles.

Media relations is a significantly important task for organizations today. Hesitation and opaqueness in media relations can backfire and consequently lead to negative stories, bad publicity and loss of customers' trust. Reputation management forum should be created at executive level, however only official representatives from corporate communications team should respond to external facing queries.

3. Identifying, Convening and Empowering the Communication Team

The Communications team has a pivotal role to play in a cybersecurity crisis situation. Communications lead along with the CEO should call upon a meeting and ensure that there is consensus within the leadership regarding the message that is shared both internally and externally.

The designated official, will be responsible for intimating the regulators via emails. The communications lead should be entrusted with preparing a media brief after due consultation with the management. The press release is an important tool to resist media furore and also to address the concerns of the board members and other stakeholders.

Professional advisors may have to be roped in as a part of the Communications team to address the employees via a board room presentation. Subject matter experts (SMEs) within the organization can schedule meeting to brief the workforce at large and alleviating any concerns that might create larger issues for management.

4. Selecting Communication Channels

Message content and channels have to be specific to the target audience. The communications channel selected for each target group should be defined by the communications lead. This can range from internal and external emails, press release for media, boardroom presentation and regulatory hearing. Shareholders' meeting and customer support services may also be channels an organization might have to adopt to stay connected with customers and other third party stakeholders.

5. Message for Target Audience

The target audience will include all relevant stakeholders arranged as per priority. Stakeholder mapping exercise should be carried out to determine the primary and the secondary stakeholders in the context of the crisis in hand. It will include, but will not limited to- shareholders, board members, employees, customers, third parties, regulators, workforce and others.

It is important that both the message and the channel be tailored as per the target audience. For instance, there will be marked difference between content that is sent out to media and the content used for boardroom presentation.

The aim of the entire exercise is to ensure that all the relevant stakeholders are informed, coordinated steps are taken for mitigation and employees are aware of the crisis without stirring panic.

6. Post-Incident Plan

A communication plan without post-incident communication is incomplete by design. While regulatory reporting, forensic investigation and other activities may definitely require significant resource diversion, it is of utmost importance to document and share, at least internally, what went wrong and why and what needs to change lest the same mistake keeps confronting the organization with likely escalating costs.[1]

[1] https://www.symantec.com/blogs/expert-perspectives/7-items-you-must-add-any-incident-response-plan

7. Regulatory Requirements

Regulatory reporting for banking organizations should be factual and must contain detailed timelines. It may include details of steps taken by the organization to mitigate the risk. In certain cases, the regulator may visit the organization to assess the impact, identify if there are any systemic risks that might arise from similar incidents elsewhere and provide guidance to the regulated entity in handling the incidents. Once a regulatory involvement is there, all decisions related to incidents should be communicated to the regulatory authority, such as related board decisions and involvements of external investigators in the incidents for maximum coordination.

7.1. Reporting to RBI CSITE (Cyber Security and IT Examination)2

The June 2, 2016 circular on Cyber Security Framework in Banks issued by the Reserve Bank of India (RBI) provides reporting requirement for banks in event of a cyber-incident to the RBI CSITE. The incidents should be reported to RBI within 2-6 hours of actual knowledge. CISOs have a clearly defined responsibility to detect breach, coordinate with the regulators and respond efficiently to minimize loss. The following Annex-3 from the circular should be used to report the incident to RBI:

- https://rbidocs.rbi.org.in/rdocs/content/pdfs/CSFB020616_AN3.pdf

The above mentioned circular mandates banks to share the Root Cause Analysis (RCA) and the potential impact of the attack on business systems.

7.2. Reporting to CERT-In

Organizations should report any adverse activity as a cyber-incident or as a cyber-security incident (as the case may be) to CERT-IN by using the following channel-

Email: incident@cert-in.org.in

Following is the incident reporting form, the format in which organizations are required to report to CERT-In- https://www.cert-in.org.in/PDF/certinirform.pdf

Once the existence of the cyber incident is established, CERT-IN will assign a tracking number and designate a team to coordinate and guide the organization.

CERT-IN, as per the urgency and impact of the crisis, will provide support, guidance and advice in identification, containment, eradication and recovery over email, phone and other channels as may be

[2] Cyber security Framework in Banks: https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=10435&Mode=0

necessary. Reporting the cyber vulnerabilities and any relevant information with CERT-IN, the format for the same is available on https://www.cert-in.org.in/. The same can be emailed to info@cert-in.org.in.

7.3 Reporting to Data Protection Authorities

In case, there is a significant data breach, which is defined as part of the crisis scenarios, the entity may be obliged to report the same as necessary under the applicable data protection legislation. For example, if the personal data pertaining to European customers is breached, relevant reporting under the General Data Protection Regulation (GDPR) may kick in. Once the proposed Indian Data Protection law comes into force, separate mechanisms for reporting of data breaches are expected to be mandated.

8. Conclusion

While effective communication is one aspect, organizations also need to keep in mind the big picture and ensure that communications records are updated and in line with the National Cyber Crime Management plan (CCMP) of CERT-IN. The CCMP of CERT-IN can be used as a reference document. Organizations should regularly conduct mock drills to ensure workability of the crisis communication plan and coordination within the organization. Periodic reviews and system audits must be conducted and proper logs must be maintained for record keeping purposes.
Organizations shall benefit from regularly attending the workshops and table top discussions conducted by CERT-IN. A member from senior management can be identified as the “Point of Contact” (POC), to coordinate regularly.

Further, organizations can refer to the Traffic Lights Protocol, explained in the appendix. The Traffic Lights Protocol is a communication hygiene framework that ensures the sensitive information is shared timely with the appropriate audience. (Please refer Appendix).

9. APPENDIX

Traffic Lights Protocol

The Traffic Light Protocol was created to facilitate greater sharing of information by employing four colors and a set of designations to ensure that information is shared with the correct audience.
It classifies the four information sharing levels –Red, Amber, Green and White

Colour	Description	Information sharing
RED	Personal, for specific recipients Information can be acted upon by named recipients only as otherwise it could cause loss of reputation and risk privacy.	Recipients may not share information Strictly restricted to participants only, not disclosed outside
AMBER	Information shared with limited recipients only and can potentially cause loss of reputation and risk to privacy is shared extensively.	Recipients can share information with members of their own organization
GREEN	Information can be shared widely among the peers for benefit of everyone in the particular industry or community	Recipients can share information with the industry and community. It still shouldn't be public
WHITE	No limit on sharing of information as the information carries no foreseeable risk on sharing	Information can be distributed without restriction, Public release in accordance to copyright laws

STAY CONNECTED

Reserve Bank Information Technology Pvt. Ltd
https://rebit.org.in

LinkedIn
https://www.linkedin.com/company/reserve-bank-information-technology-pvt-ltd

Twitter
https://twitter.com/reservebankit

Email
communications@rebit.org.in

ABOUT REBIT

Reserve Bank Information Technology Private Limited (ReBIT), has been set up by the Reserve Bank of India to serve its IT and cybersecurity needs and to improve the cyber resilience of the Indian banking industry.

CYBERSECURITY PLAYBOOKS

The Cybersecurity Playbooks are designed to provide step by step instructions to implement a specific process or control within an organization. These playbooks have been developed specifically to assist the banking sector implement the security controls effectively.

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. ReBIT disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any act or omissions made based on such information. ReBIT does not provide legal, regulatory, audit or tax advice. Readers are responsible for obtaining such advice from their own legal counsel and other licensed professionals.

No part of this publication may be reproduced, adapted, stored in a retrieval system or transmitted in any form by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior permission of the author.

Subscribe to ReBIT's Cyber Pulse Monthly Newsletter

https://rebit.org.in/newsletter