2022

Cyber Crisis Communication – A important factor in Incident Response

A high-level Approach

SUNIL VARKEY

Overview

The noun **crisis** comes from the Latinized form of the Greek word krisis, meaning "turning point in a disease." At such a moment, the person with the disease could get better or worse: it's a critical moment.

In the current turbulent cyber terrain, a crisis is not a 'one of' 'once in a while situation considering the interconnected inter-dependent environment we operate. An incident on an entity has a ripple effect on so many other entities and stakeholders globally, considering the federated nature of business.

In our digitalized social media era, it is difficult to suppress a cyber attack or crisis for long; it is essential and better for the organization to be proactive in communicating rather than leaving constituents to interpret situations in their way.

In the past, we have seen different approaches taken by organizations in crisis communications,

- A senior leader with no sensitivity to security handling a journalist, just promising that the forensic investigation report of the incident will be made public - creating more confusion for stakeholders
- A leading IT vendor open and transparent on the incident, and updates were communicated frequently on their understanding, actions and mitigation approach.
- A large service company silent on their negligence impacting its customers
- Blame games and irrelevant information

Each of these approaches has its own merits and demerits.

Many enterprises had damaged much more significant than the actual cyber incidents by unprofessional, non-transparent communications and statements on specific events.

Effective Communications and narratives are essential both in peacetime and crisis time. Every entity needs to be prepared to handle a cyber crisis scenario at any time in which inward and outward communication is a crucial aspect. Handling crisis situations (pre, during, post) with transparency, confidence and empathy during the worst period helps build trust and confidence for long-term relationships.

Crisis communication refers to the technologies, systems and protocols that enable an organization to effectively communicate during a major or significant threat to its business, reputation or stakeholders. It is also a prepared, honest and responsive approach to sharing information intended to improve constituent perception in an adverse situation assuring organizational Readiness, Response, Reassurance, and Recovery commitment.

Interested parties and Constituents

Multiple stakeholders, both internal and external, are interested (for good and bad) parties on events that impact enterprise sustainability and affect its constituents.

From an external stakeholder perspective, it could be

- customers,
- partners,
- regulators,
- competition,
- supply chain,
- media,
- researchers,
- insurers,
- enviers,
- fraudsters, Adversaries

From an internal stakeholder perspective, it could be

- employees,
- management, board, Audit Committee
- Specific internal stakeholders are
    - CEO
    - CRO
    - GC
    - Company Secretary
    - CMO
    - COO
    - CFO
    - business/account leaders

Many regulators and contracts mandate communication and disclosure of any incidents.

For each of these internal and external stakeholder groups, specific, clear need-to-know basis communications are required at different stages of an incident crisis. Without defined policies for disclosure and designated participating stakeholders to execute, it is not practical for a single stakeholder group to communicate with all with relevant information, considering various communication formats, depth of disclosure, and language to each recipient group in the specific time frame during a crisis.

Cybersecurity is a niche domain, and every crisis can be different. Most stakeholders may not clearly understand security controls and types of incidents, except the hyped word of 'breach' in a single context. And each of the stakeholder groups expects communication which is relevant, contextual, and understandable to them to consume and take it forward.

During a crisis, considering the existence of

- possibility of grapevine
- deformation attempts by different groups through social media
- media coverage without facts
- new attack campaign adversaries
- Assurance sought by stakeholders and customers
- Regulatory pressure

All official crisis communication is to be worded to clarify and avoid speculations.

Speculative, suppressed, non-confident, denial without rationale, and too-much or too little disclosure in these communications can have its problems.

It is normal to observe multi-fold attack attempts, malintent blogs, wisdom-sharing groups, tutorials for further attacks, customer pressure, and speculations during a crisis, mainly based on non-validated information shared by internal stakeholders, speculators, or advisories.

One of the challenges faced in my earlier SOC role was that during an incident, a technical handler working under pressure to handle (validate, contain and mitigate) the incident was mandated to face stakeholder teams periodically to upraise the situation.

Pureplay technical resources (not customer-facing role in the idle situation) under crisis pressure struggled to build trust with their stakeholders confidently. An alternate approach we used at that time was to involve a group of SOC resources with technical call centre experience, fluent in English, and trained in handling pressure to interact (bridge, calls) with external stakeholders with the details provided by SOC technical handlers. It was a game-changer in reducing the additional stress on incident handlers while working on the crisis.

This is a reality in many security crises where CISO is mandated by internal business and functions to face external stakeholders since no other internal functions take up the role or are ignorant of what is required. With these mandates, CISOs lose valuable time in crisis mitigation.

Hype and Trust

Media and others overhype 'Breach' as a term; any incident (of any nature) related to cyber is termed 'Breach'. This hype creates considerable damage and a multi-fold impact on enterprises. Many take advantage of this situation since it is not viable for any enterprise to come out promptly to clarify the situation and arrest speculations during a crisis.

Also, it is too challenging to identify who is your partner and friend during a time of crisis. There were many situations where a partner, contractor, vendor, or consultant working with you leaked sensitive non-validated information to external parties or their communities for fame (or other interest), worsening the crisis.

Approach

During crisis phases, the enterprise needs to have a common sustainable approach in crisis communication to its internal and external stakeholders. However, content details may vary for each of the stakeholder groups.

The crisis communication approach should be a defined and tested process in the enterprise incident handling program, and this has to be periodically updated, tested and signed off by legal and corporate functions.

The cyber crisis is slightly different from BCP-DR since

- nature and impact may vary in each of these crises,
- the effect may or may not be visible fully,
- external/internal adversaries are involved,
- response recovery process always not be of the defined one in the document.
- Highly dynamic in nature with motivated adversaries behind the scene changing tactics

One of the suggestive approaches to crisis communication is

- Create a program for crisis communication within CISO's organization, which is a continuous activity considering changes in approach, stakeholders etc
- Define internal and external stakeholders based on the level of information they should be getting and the periodicity during the incident
- Define the method and frequency of communication to each of these stakeholder groups
- Build a Crisis communication playbook

Challenge

Assume a situation of a critical cyber incident; to avoid lateral movements and their impact, you may have to isolate a few networks, suspend service or isolate an office location. CEO needs to be informed for their concurrence; you call and wake up CEO from sleep at a late hour, brief them the situation and ask permission to disrupt operations to avoid a further significant impact or to avoid additional damages. In that short time, CEO will be clueless (except on the trust in CISO) on how to validate, weigh options and provide approval; he may not even have valid questions to clarify his assumptions properly.

Decision-makers and authorities during a crisis have to be pre-defined, and they should have the required know-how to take the decision.

Crisis Communication playbook

The objective is to define - What to communicate, When, to Whom, How and Why and by Who – when time is critical, information is limited, mounting pressure for various stakeholders updates, and answers to all questions (who, what, why, when, where, how)are not available.

Define 15-20 different **Cyber Crisis scenarios** based on the business and security maturity – a few examples

- *Malware propagation*
- *Ransomware*
- *Sensitive information leaked to public space*
- *Privileged credentials available on the Dark web*
- *DDOS*
- *Vulnerability disclosure of an internal system in the public domain*
- *Massive recon activity – coordinated across multiple internet gateways*
- *Presence of rootkit on multiple critical servers*
- *A considerable volume of data extrusion attempts*
- *PII / PHI data leaked*
- *Breach disclosure in media and social networks*
- *Attacks (malware, phishing, DDOS, recon, exploits) originating from the internal network to outside networks and federated connections*
- *Lateral movements*
- *Account takeovers*
- *Service disruptions*
- *Targeted massive phishing campaign*
- *Misconfiguration in cloud workloads, leaks*
- *Leveraging internal network for external attacks*

Define internal and external stakeholders (participative/informed)

- Participative: CIO, CRO, COO, CMO, DPO, CHRO, GC, Company Secretary, CEO, Business / functional leaders, external threat intelligence bodies, partners etc
- Informed: employees, partners, helpdesk, regulators, customers, CERT, law enforcement, Media, insurers, supply chain, impacted parties etc.

Roles and Responsibilities

For each of the participative roles, their responsibilities are to be defined.

- Specify their role in each of the defined incident scenarios
- All may not have a role in every incident scenario, and some may have a role in all scenarios. Ex. DPO / Privacy officer role is only required if the incident is related to GDPR, PII, PHI (depending on the regulation and policies)
- Define around five questions (based on the incident scenario assigned) they could ask to get the context and clarity of the incident (will get answers during the crisis from the central team)
- Questions to be agreed upon during the planning stage and further refined during testing and changing the environment
    - Else time will be wasted during the crisis with vague general-purpose questions from each of the stakeholders

During a cyber crisis, CISO will be in charge of Crisis management.

- Participative stakeholders will have assigned target recipients groups to which only they should be interacting (ex. CMO to Media, ex. DPO to privacy regulators, CRO to board etc)
- Guidelines on what (not) non-participative stakeholders (employees, contractors, partners) can share during and after the incident.
- Language, min/max information to be shared at each phase of the crisis with respective stakeholders (external and internal) to be defined and documented.
- This is to be signed off by respective leadership stakeholders, and compliance adherence should be mandated.
- Information shared should be specific to avoid different interpretations
- Classification, RMS / Encryption enforcement based on the sensitivity of information shared with specific groups.
- All 3rd parties involved in the incident should have NDA signed.

Methods and mode of communication varies; some of the examples

- Email
- Bridge/virtual hosted calls
- Internal portals
- Collaborative tools
- Social Media
- Calls
- Bulletin boards
- Service desk
- Out of band

Updated Response content template for each defined crisis scenario in each incident phase to be available in the playbook.

Designated individuals or functions within CISO's team should ensure the required information is available to each participating stakeholder during the crisis, as defined in the playbook.

The playbook should be updated annually when roles or situations change or based on learnings.

The playbook should be available and accessible to all participating stakeholders when required.

A tabletop exercise is to be done every six months, and full-blown testing must be done yearly for this to be effective.

Bad crisis communication could have a ripple effect of bad communication, attracting new attackers, lost customer confidence, reducing stock price, employee/partner morale etc.