Cybersecurity & Crisis Management

Key Stakeholders & Their Priorities →

LESTER CHNG

Imagine for a moment.

Your company is hit with ransomware.

You are the incident/crisis lead.

Your CISO calls for a meeting and you are facilitating.

Almost all the teams are represented at the meeting.

Each team will have its priorities.

Knowing the priorities of these teams below will prepare you for the questions and allows you to help control the narrative.

Legal
C-suite
Business
Technology
Cybersecurity
Privacy office
Public relations
Regulatory liaison
Federal authorities

Here are some priorities and questions that you may face.

LEGAL

Priorities

- Reducing liability
- Fulfilling legal obligations to clients, partners, and authorities
- Use of appropriate language

Questions

- Do we have confirmation of a cyber incident?
- Who is currently aware of this incident? We will want to restrict that information flow.

C-SUITE

Priorities

- Projection of confidence
- Reputation management
- Business continuation
- Legal liability

Questions

- Do we have the correct expertise and support to handle the incident?
- What are some pro-active steps we can take to prevent further damage?
- Are we allowed to pay the ransom?

BUSINESS LEADS

Priorities

- Business continuation
- Customer/Client relations

Questions

- What can we disclose to our top clients? They are asking us for details
- What are the impacts to business and what processes can continue?
- How quickly can we resume business as usual?

TECHNOLOGY

Priorities

- Operations continuation
- Impact to other technology

Questions

- What is the extent of the malware?
- Are we able to isolate it and recover on our backups?
- Will our mitigations be effective?
- Will we get re-infected?

CYBERSECURITY

Priorities

- Assessment of full impact
- Mitigation of damage
- Containment and recovery

Questions

- Are we able to continue our threat hunt and investigation, we want to have full assessment of damage
- Can we get more time to run forensics?

PRIVACY OFFICE

Priorities

- Breach of information
- Regulatory obligation

Questions

- Are we able to confirm if we have exposure of personal data?
- Are the actions we are taking able to limit further loss of such information? if we wont get re-attacked?
- Can we get detail numbers and type of information loss

PUBLIC RELATIONS

Priorities

- Reputation management
- Projection of confidence

Questions

- Can we get the latest updates?
    - investors and media outlets are awaiting info
    - Social media reports are trending, we need the updates to control the narrative

REGULATORY LIASION

Priorities

- Regulatory obligations

Questions

- Are we able to confirm if there has been loss of information?
- What is the extent of the impact?
- Does it affect our customers in other countries?
- Have federal authorities been informed?
- What steps have we taken?

FEDERAL AUTHORITIES

Priorities

- Investigation and evidence

Questions

- Have we been in contact with the threat actor?
- Have we captured all the evidence of the incident?
- Have we informed our industry partners and other federal agencies?

YOU CAN DO THIS TODAY

Identify the key stakeholders

Undertand their priorities

Establish a central point of communication

Establish a cadence of reporting

Prioritize and maintain control

Want to learn more about cybersecurity and crisis management?

FOLLOW ME ON LINKEDIN @LESTER CHNG