DYNAMIC CRISIS RESPONSE: *MANAGING THE BREAKING CYBERATTACK STORY*

RUSS MCREE

MICROSOFT SECURITY RESPONSE CENTER

Precedent…the lack thereof

2020 proved to be a watershed year with evolving cybersecurity threats, 2021 is proving to be no better…

There is a continuing rise in the determination and sophistication of nation-state attacks

The growing privatization of cybersecurity attacks is akin to 21st-century mercenaries

Prepare

Treat crisis communications for what it really is…an Emergency Support Function

Group capabilities into an organizational structure to provide support, resources, and services needed to protect your organization, restore essential services and critical infrastructure, and help return to normal following incidents

Crisis communications are central to this endeavor

Priority

A crisis communications team should be prepared to coordinate, collaborate, cooperate, communicate for…

- External proactive messaging
- External reactive media and talking points
- Customer escalations
- Customer notifications
- Review and contribute to field notifications
- Review and contribute to blog and content generation

Inform

Need to know (NTK) is mission critical

In the absence of NTK, there will be leaks, and control of the message will be lost…

- External messaging must be centrally managed
- No one talks to the media without explicit approval
- Manage and monitor social media
- Refer external media inquires to your communications team

Notify

Interaction with government agencies is unique, dynamic, situational, and challenging

- Keep your lawyers close by
- No one talks to government without explicit approval
- Enable programs to facilitate government interaction (GSP)
- Trust through transparency and confidential security information for qualified governments
- Enables controlled access to source code, exchange of threat and vulnerability information

Data

Data informed decisions must prevail

“Universal law is for lackeys; context is for kings.”

- Breach and compromise details can be nuanced
  - Were customers impacted?
  - Is a vulnerability being actively exploited?
  - Are there mitigations to enable immediate protection?
  - Who is the adversary?

Issues

Issues management shapes media and press communications for breach response

- Prepare talking points
- Be timely
- Neither under-inform, nor exaggerate
- Truth and consistency matter
- Update as appropriate
- Provide closure

russ@holisticinfosec.io
rmcree@microsoft.com

@holisticinfosec
https://holisticinfosec.io/
@msftsecresponse
https://msrc-blog.microsoft.com/