How Management Absorbs Information During A Cyber Event

SANS Data Breach Summit 2018

BREAKING NEWS

Breach of D

The Beginning

- Leadership will be looking for answers
- Set the tone out of the gate
- Give leadership confidence in what's happening
- Demonstrate that the security team will drive

Everything is about communication

Shape the Story

- Every incident has a story
- Immature organizations look for a scapegoat in an incident
- Get ahead of the media
- Leverage your organization’s public relations to shape the story

Manage Expectations & Communicate Regularly

- Communicate
  - *Who will provide updates*
  - *How updates will be provided*
- Set a schedule for updates
- Provide updates whether or not you have them
  - *Use time to reiterate facts*
  - *Reiterate what's being done*
  - *Answer questions*
- Leverage an open bridge line to convene leadership quickly
- Don't assume anyone remembers what you told them previously

Use mechanisms that are reliable and predictable for leadership

Maintain a Knowledgebase

- Data evolves rapidly in an incident investigation
- Identify who needs the facts
- Make access to the latest facts easy; utilize multiple approaches
  - *War room with facts on white board*
  - *Document share site*
  - *Fact sheet*
- Put expiration dates on the top of all written fact documents
- Clearly delineate what is public information and what is confidential
- Remind everyone at the beginning of every meeting

Take Care of Your People

- Senior leadership will be expecting a lot from the security team
- Productivity and quality will suffer when people are too stressed and haven’t slept
- Health incidents can happen in high stress situations
- Put a back-up plan in place; set the example
- Demonstrate to leadership that they will get what they need

Prepare in Advance

- Conduct table top exercises
- Establish, communicate, and test escalation Procedures
- Identify people with strong communications skills and engage them
- Create central storage location for incident information and test access
- Establish, communicate, and test a clearance process for information release
- Know what you have visibility into and your log retention
  - *communicate in advance what you would/wouldn't be able to provide in an incident*
- Know what your regulators and contracts require for reporting

Meet “Ted”

- Ted is a senior leader and he’s really jazzed by the appeal of the incident
- Ted wants to learn all about security and get to know the team
- Ted has a dinner party tonight and he’d like a few juicy pieces of technical info to use to impress his guests

…Ted asks you to add him to the technical bridge so he can have *the* latest on the incident

No, Ted.

The “Ted” Approach

- Explain things to Ted in business terms
- Make sure you give Ted information or he will look for it
- Give Ted face time with security leadership
- Prepare Ted to speak about the incident
  - *Give Ted stories he can tell*
  - *Give Ted talking points*
- Ask Ted to help you

Meet “Sue”

- Sue is your company’s security leadership
- Sue came up a technical track and hasn’t been in the role long
- Sue has never handled a situation like this and she is struggling with the business leaders

The “Sue” Approach

- Feature an Incident Commander or other leader
- Position Sue to participate where she shines best
- Prepare Sue as much as possible; help her think through leadership questions
- Make it clear to other leadership that while Sue might not be a savvy business leader like them, her team works together to get the job done

Meet “Ron”

- Ron likes to be the guy with the info
- Ron is looking for facetime with leadership
- Ron keeps taking pieces of information to leadership before you
- Ron regularly contradicts the facts in meetings

The “Ron” Approach

- Communicate & reiterate escalation procedures
- Make the facts readily accessible to those that need them
- Talk to leadership about the importance of information flow to avoid inefficiency and confusion
- Give Ron a role to play in the incident

Meet “Allen”

- Allen is legal counsel
- Allen is concerned about sharing information publicly until all facts are established
- Allen is concerned about the regulators knowing too much
- Allen is concerned about being in breach of contract with partners

The “Allen” Approach

- Engage Allen in the process so he knows nothing is being withheld
- Demonstrate precedent at other organizations
- Establish a clearance process for release of information
- Engage other leaders with influence
- Engage a leadership team in key decisions so Allen doesn’t need to trust only one person

After the Incident

- Continue communications with leadership
- Involve leadership as you address items identified in the after action report
- Share your experience with other organizations; have your organization be seen as a responsible thought leader

Never let a good crisis go to waste!