Now What?

A Pragmatic Approach to Effective Breach Response for Leaders
About Me

• CISO @ Federal Reserve Bank of Atlanta
• Certified Instructor @ SANS Institute
• Handler @ Internet Storm Center
• @russelleubanks
Outline

• What’s on your mind
• Obligatory Quote
• What you need
• Always
• Never
• Leaders role
• Stakeholder Management
• Golden questions
What’s on your mind?

Kübler-Ross Grief Cycle

- Denial: Avoidance, Confusion, Elation, Shock, Fear
- Anger: Frustration, Irritation, Anxiety
- Depression: Overwhelmed, Helplessness, Hostility, Flight
- Bargaining: Struggling to find meaning, Reaching out to others, Telling one’s story
- Acceptance: Exploring options, New plan in place, Moving on
“There are only 2 types of Leaders: Effective and Ineffective"
What you need

• A healthy dose of “Always”
• A healthy dose of “Never”
Always

• Determine and communicate the next meeting
  – Each call
  – Each meeting
Always

• Assign names and deadlines
Always

• UNODIR this is their priority
Always

• Expect the unexpected
Always

• Be respectful
Always

• Be open to being wrong
Never

• Assume the team to knows your expectations
  – Work through the weekend
  – Wait until Monday
Never

• Believe the schedule is perfect
Never

• Underestimate the value of rest for your team members
Never

• Expect the breach will remain private
Never

• Make promises you can’t keep
Leaders role

• Ensure proper expectations of your team members throughout
Leaders role

• Categorize the breach
  – L/XL/2XL
Leaders role

• Be prepared to be wrong
Leaders role

• Decide who is second in command
Stakeholder Mgt

- Key to success is to knowing their expectations
  - In advance
Stakeholder Mgt

• Up
• Down
Stakeholder Mgt

• Human Resources
  – Comp time
  – Overtime
  – Creative Compensation
Stakeholder Mgt

• Legal
  – Protect
  – Obligation
  – Report
Stakeholder Mgt

• Physical security
  – Restricted areas
  – Press
  – Employees
  – The curious
Stakeholder Mgt

• External
  – Government
  – Regulators
  – Auditors
  – Law enforcement
Stakeholder Mgt

• Cyber Insurer
  – Notification requirements
  – Update requirements
Operating model

• Very incomplete evidence
  – Leaders operate here regularly
    • Strategy
    • Hiring
    • Incident Response
  – This can be leveraged
Golden questions

• How do I think about this?
Golden questions

• What are the current blind spots?
Golden questions

• What are other possible conclusions?
Golden questions

• Where is there lack of agreement within the team?
Golden questions

• Fact Based?
• Fear Based?
Golden questions

• What would a great leader do?
Your Questions