Breach Response in a Crazy World

Matt Bromiley
Incident Responder & SANS Instructor
TAKEAWAY 1

KEEP CALM
THIS IS FINE.
This is fine.
Recipe for Disaster

Your IT team
- Intimate knowledge of environment
- No time to answer questions

Lawyers and consultants
- Knows nothing
- Bills hourly

C-Suite/BOD
- Wants answers yesterday
- Does not comprehend situation
Keeping Calm Let’s You

• Manage the incident
• Manage your team
• Keep others calm
• Make smart, informed decisions
• Deal with whatever comes your way
TAKEAWAY 2

GO BACK TO SCHOOL
EVERY BREACH IS A LESSON LEARNED
EVERY BREACH IS AN INCIDENT
ADWARE
RANSOMWARE
TAKEAWAY 3

COMMUNICATION
IF YOU COULD ATTEND...

THE HOUR LONG MEETING AT 1630
External Communications

Dos

- Talk to counsel first.
- Appoint key people to talk externally.
- Be prepared for questions.
- Be honest.

Don'ts

- Answer questions you don't know the answer to.
- Give away more than you have to.
- Guesstimate or be vague with the intention of CYA.
- Withhold from law enforcement.

MAKE THE MOST OF A BREACH
Internal Communications

Dos

- Involve ALL the necessary people.
- Tell your executives.
- Stress confidentiality and/or privilege.
- Designate point people - they will talk.

Don'ts

- Hold meetings every hour.
- Involve unnecessary teams.
- Segregate in the name of productivity.
- Dismiss any plausible theory.

MAKE THE MOST OF A BREACH
TAKEAWAY 4

MAKE THE MOST OF A BREACH
STEP 1: GET BREACHED
STEP 2: $$ PROFIT $$ $$
STRENGTHS AND WEAKNESSES

MAKE THE MOST OF A BREACH
Strengths and Weaknesses

• Watch your teams during a breach – **the most knowledgeable will rise to the top.**
  • Make a note of these employees. They should be involved in the next IR plan discussion.
  • These are your next team leaders or “go-to” people (if they aren’t already)

• **Your organization is opening previously-closed channels of communication**
  • Take advantage of these, and let them live beyond the breach.
Strengths and Weaknesses (cont.)

• Watch out for team failures and weaknesses – **these are your priorities after remediation.**
  • Identify difficulties in communication, approval, or knowledge gaps.
  • What can we do to solve these problems **ASAP?**

• **Allow symbiosis and progress to occur.**
  • Your employees don’t want to live this way for ever. Let them find (safe!) ways to get things done.
  • Don’t micro-mange.
Strengths and Weaknesses (cont.)

- Remove hurdles quickly.
INCIDENT RESPONSE PLAN

MAKE THE MOST OF A BREACH
Incident Response Plan
Incident Response Plan

• Got one – **USE IT!**

• Print it out and keep it on you at all times
  • Make edits where you fail, highlight where you succeed
MAKE THE MOST OF A BREACH

IMPROVEMENTS
MAKE THE MOST OF A BREACH
Improvements

Wish list == purchase orders.

Take advantage of the spotlight
• Don’t be irresponsible, but now is the time to get your security in a better place.
• Remember those top performers? Talk to them.
• Listen to external parties.

MAKE THE MOST OF A BREACH
CONFERENCE TAKEAWAYS
Conference Takeaways

• Call external counsel
  • Attackers are not stopping, so breaches are not stopping
    • Patch, patch, patch
    • Develop an IR plan
  • Develop an IR plan, think about continuity/recovery
  • Assess who from the org is on your response team
    • Know when you need help – and ask for it
  • Watch the news – be aware of this crazy world.
    • Get some rest – you’re going to need it.
THIS IS FINE.
A HUGE thanks to all of our 2017 Data Breach Summit speakers and attendees.

This year was a huge success thanks to YOU!