Practical Tabletop Drills for CSIRTS - Pre-session Material

FIRST Annual Conference
Edinburgh, Scotland

June 2019

KRvW Associates, LLC
Ken van Wyk, ken@krvw.com, @KRvW_Associates

IRTs need to play with others

To name a few

- Human resources
- Communications
- Legal counsel
- Executive decision team
- Business owner
- Customers
- Government regulators
- And so on…

They ALL need to be ready

Design vs. Implementation

Your success or failure may well be determined by the actions of others

Now do you think they're all ready?

How do we prepare them?

- Different approaches
  - Train the entire team
    - SOPS, their roles, their responsibilities
  - Practice your processes
    - Drill, drill, drill!

Emergency preparedness drilling

It is not enough to merely practice until you get something right

Instead, practice until you cannot get it wrong

Keys to success

You will need

- All the stakeholders
  - Leads or designees from each organization in the entire CSIRT plan
- A few realistic scenarios
  - Don't forget the business
- A half day
- Facilitator
  - Best if facilitator isn't a participant
- Planner
  - Someone to plan and write the scenarios

Planning the scenarios

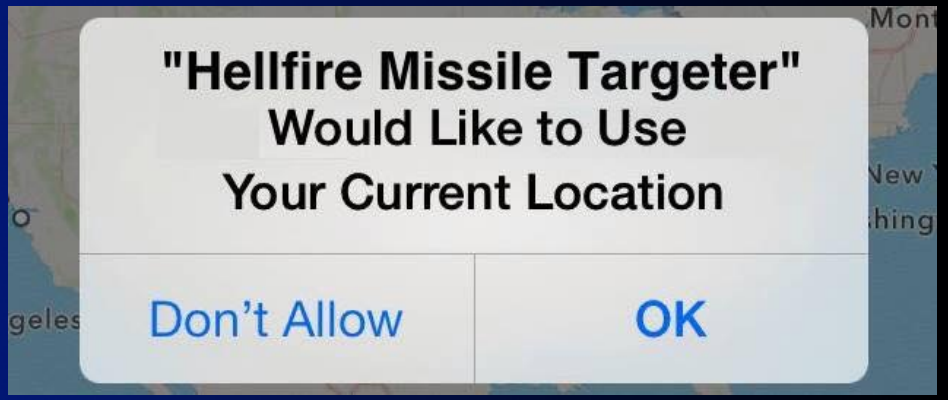
- Considerations
  - Business nightmares
  - Involve the team to learn about the landscape
  - Realistic and topical
  - Don't share the scenarios
- Each scenario should run for about an hour
- I generally build 3
  - 1 to practice (think: training)
  - 2 more to push the limits

Business nightmares

- Deep understanding of the business
  - Priorities and concerns
  - Strengths and weaknesses
- Now, what are the technical shortcomings
  - Signature-based protections
  - Business hour monitoring
  - Not everything monitored
- Limit sharing of scenarios

For this session…

- A company
- Company and CSIRT background info
- Company priorities
- Roles and descriptions



The Players - Snake Charmer

Snake Charmer, Inc.

- Publicly traded, USD$3 Billion company
- Software as a service company
- COBRA is its flagship software (more on that in a moment)
- Built over years as a data center model application
- Customers connected via web browser, mobile, etc. to SC's servers
- Recently went public and hired a new senior executive team
- Executives brought in to reduce costs and improve scalability of the COBRA platform

The Players - COBRA

COBRA is the company's proprietary software

- It is used to organize, optimize, and manage very large-scale industrial projects such as building corporate campuses, military bases, and such
- It tracks hundreds or thousands of sub-contracted projects and providers
- Administrative tasks like invoicing and payments
- Project management tasks like milestone and schedule management
- Their "special sauce" is COBRA's ability to look across vendors and projects for cost savings and other optimizations
- It is the market leader in the niche field of delivering huge industrial projects
- Massive scalability has been a big challenge, however

Company background

New management team is convinced their future lies in the cloud

- Selected upstart cloud provider, Elbonian Web Services (EWS)
- Deployed COBRA to EWS last quarter
- Still working out the kinks a bit, but they are now operational on EWS

Incident response

SC has a fairly mature IR process they have adapted to the new EWS environment

- SOPs for most workflows (more on that in a bit)
- SOC provided by EWS for 24/7 tier-1 monitoring and support, including IT and security hotlines, ArcSight SIEM, Splunk
- Although tier-1 is at EWS, SC retains overall responsibility and management of the IR process
- Tier-2 and Tier-3 are handled in-house at SC

Standard Operating Procedures

SC has a simple, but foolproof set of SOPs for incident detection, triage, and escalation

- Incident severity levels: LOW, MEDIUM, HIGH
  - LOW is localized and/or easily resolved by IT staff with little or no business interruption
  - MEDIUM incidents can impact multiple systems and potentially spread, but business impact is still viewed as minor, with no PII or proprietary information breached
  - HIGH incidents are large in scope or involve PII, customer, or proprietary data exposure
- Tier-1 SOC receives incident reports
  - Validate info, triage incident, and handle LOW incidents
  - Escalate to Tier-2 any MEDIUM incidents within business day (weekend incidents can wait until net biz day)
  - Escalate to Tier-3 any HIGH incidents 24/7 within 30 minutes
- Escalation includes hand-off of all data collected about incident including packet data, Netflow, phone logs, emails, and any other data collected
- Tier-2 or Tier-3 assume operational control (OpCon) at that point

The Roles - and volunteers?

CISO - Reports to Board of Directors
CSIRT Manager - Reports to CISO
SOC Tier-1 - Works at EWS, but reports to CSIRT Manager
Company Tier-2 - Reports to CISO, except for incident ops
Company Tier-3 - Reports to CISO, except for incident ops
Business Owner - Reports to COO
COO - Reports to CEO and Board
General Counsel - Reports to Board
Communications - Reports to CEO
CEO - Reports to Board
Major Investor - Largest external shareholder

Process

I will introduce the events (aka "injects") as they occur, along with timeline

- Basic data will be on slides

You respond as you would expect to

- Discuss process
- Ask operational questions
- Take actions as appropriate

Ready to start?

Kenneth R. van Wyk
KRvW Associates, LLC

Ken@KRvW.com
http://www.KRvW.com