Incident Response

Pushing your CSIRT or PSIRT to its limits with tabletop drills

KRvW Associates, LLC

Ken van Wyk, ken@krvw.com, @KRvW

What's the problem?

Your CSIRT is up and running, but…

- Maybe things didn't go as you'd expected during an incident
- Senior management still doesn't really "get it"
- You simply want to ensure you'll be up to a big incident

Let's try to prevent failure

- Always best to optimize the odds in our favor
  - After all, we need to justify the value of having a CSIRT in place
- The CSIRT mission should include minimizing the adverse impact of security crises

Total perspective vortex

- It's all about the business
  - Not the technology
  - Yeah, that's a tough pill for technologists to swallow
- Tech goodies are merely tools for doing the job

CSIRTs need to play with others

To name a few

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

Technical excellence is not enough

- You've hired a top-notch tech team
- You've purchased and are maintaining the best tools
- Your team is constantly abreast of the threat landscape
- These are great, but not enough

Of course you have a plan

You've written, edited, and fine-tuned an incident response plan

It spells out every process you can expect during a crisis

That's not enough either

You're ready for anything

In short, you think your team is prepared

Are you willing to stake your reputation on that?

Consider this

Your success or failure may well be determined by matters outside your control

Now do you think they're all ready?

Consider: Did everyone read the plan?

- All those folks you need to work with, that is
  - Did they read it?
  - Will they know what to do during a crisis?
  - How confident are you in that?

How do we prepare them?

Three things you can work on

- Train the entire team
- Practice your processes
- Verify things are working how you want them to

Is it possible to train them all?

Not likely, so…

Train them without them knowing you're training them

Bring on the tabletop drill

- Tabletop drills can train and test at the same time
  - But you have to do them right
  - Some of what you find out you will not like
  - But, in the end, you'll be better off for it

Keys to success

You will need

- All the key 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
  - 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

Build a timeline of each scenario

- Start at the beginning
  - What happens and when
  - Be realistic with times
  - Incidents occur 24/7
- Build each scenario in its entirety
  - Play it out in your mind
- Be prepared to be a bit flexible

Construct a slide deck

- Series of event "injects"
  - Each slide should have a time and an event
  - You're describing what happens, not the responses
- Avoid branching if possible

Example injects

For your consideration

- Malware detected on PC
- TV news crew ambushes company CEO in the parking lot, demands answers
- Desktop security software failed to identify any malware

Setting the rules

- Tabletop drills need to be carefully planned and executed
  - Participants need clear guidance on the rules of engagement
  - Someone needs to ensure compliance with these rules

Cyber range time

- What you'll need
  - Projector
  - Whiteboard
  - Notes
- Proceed one inject at a time
- Allow time to respond
  - Questions, discussions
- Do not lead them!
- Take good notes of actions

Immediate wrap-up

- Summarize the incident and actions taken
  - Questions and discussions on what took place

Hot wash each scenario

- What worked? What failed?
  - Constructive criticism of failures
  - How can we improve?

Common failure points

Look for these (and more)

- Who was in charge?
- Communication breakdowns
- Single points of failure
- Evidence handling
- Overly optimistic time lines
- Do everything possible
- Prioritization

Consider a simple example

- Company identity removed (I hope)
- This one is designed to warm the group up and introduce the tabletop process
- The next scenarios should push much harder
  - What kind of incidents would the CSIRT have the most difficult time resolving?

Time - 06:00-09:00 (EST)

It's early Wednesday morning, and things appear to be mostly "business as usual" at XXX.

Corporate Communications team is going through early morning news updates on web sites, social networks, etc.

They log in to social network recruiting account and post a small number of customer-facing news updates for the day

- Logins are done from staff home machines, connected to XXX over VPN connections

Time - 08:00-09:00

XXX IT Security reviews their daily threat updates:

- New Chrome patch issued by Google
- US-CERT bulletin regarding recent Windows “patch Tuesday” updates
- Twitter security team says they’ve fixed the “clickjacking” vulnerability that was actively being exploited last night on several social media sites
- Desktop Security team announce signature updates available for several new malware and virus reports
- IDS team posts alert signatures for patch Tuesday, Chrome exploit, and Twitter “clickjack" exploit
- Various other product security update postings

Time - 09:15

XXX's web support group gets "Contact Us" message from customer saying:

"*I demand you immediately stop sending me all of these obscene messages, or I will report you to the authorities!*"

Person leaving message leaves a fake email address so contacting him/her is not feasible

Time - 09:30

Company receives numerous additional "*stop sending me this stuff*" messages via the Contact Us feature on web site

They largely go unnoticed, as the person who normally checks these messages only checks them a couple times a day

Time - 10:30

XXX employee who checks the Contact Us queue logs in to find several dozen “stop sending” messages

Immediately sends the messages to the IT help desk and reports:

“*We’ve been getting several of these messages via the XXX web site, but I have no idea what they’re referring to. Since we’ve gotten so many of them, I thought I’d bring it to your attention.*”

Time - 10:31

XXX's IT Security begins its investigation into the source of the customer messages.

From the "Contact Us" information forwarded, the IT Security team sees several dozen email accounts, some real and some are obviously fake, but no other log or even helpful data.

Time - 11:30

A few executives from XXX leaving for a lunch meeting are ambushed outside the front door by TV news crews.

A TV reporter recognizes CEO Wile E. Coyote and asks him, on live camera, "*What can you tell us about the hacker attack that has hit XXX? Is it true that the hackers have hit some of your financial transaction systems?*"

Mr. Coyote, unaware of any security breaches, waves them off and says, "*NO COMMENT*" as he climbs into his car and speeds off for his lunch meeting.

Time - 11:31

Mr. Coyote calls IT security and tells them about the news crew ambush and instructs them to fix the problem *immediately*

Time - 11:45

Corporate Communications department starts fielding numerous phone calls and emails from local media outlets regarding “the hacker incident”.

With no information available yet, Corporate Communications team does their best to fend off the media for now.

Time - 12:00

Corporate Communications calls IT Security. After call from CEO and media inquiries, they checked, among other things, their Twitter account and found several highly inappropriate messages had been posted from it, so they've changed their password.

They're not sure how attackers could have gotten their Twitter account password, but they changed it just to be on the safe side.

Time - 12:30

The Security team reviews IDS alerts and network logs and finds no indication of any out of the ordinary traffic.

One anomaly does stand out, though. Several employee home PCs show abnormal amounts of outbound traffic to https://twitter.com

- The home PCs were connected to the corporate network early this morning via VPN

They verify the home PCs are owned by multiple employees in Corporate Communications

Time - 13:00

What happens next?

What actions can and should be taken? By whom?

Hot wash

Overview of incident big picture

What worked well?

What didn't work so well?

Any concerns for your organization?

Were you appropriately engaged?

How did the media get involved?

In what ways did media and the CEO's involvement change the dynamics of the incident?

What complicating factors hindered our IRT?

Note what's not in the scenario

- The scenario doesn't say how the messages were posted
- No indication of what the CSIRT should or did do
- No outcome either
- How did the local media find out?
- Scenario is top-level details only

Kenneth R. van Wyk
KRvW Associates, LLC

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