Table Top Exercises (TTX) & Cyber Drills for Increasing Incident Response Preparedness

Adli Wahid

adli@apnic.net

Let’s Connect!

- CERT/CSIRT engagement, Security Community & Honeynet Project @APNIC
- LinkedIn : Adli Wahid
- Twitter/Insta: adliwahid
- Email: adli@apnic.net

Today’s Plan

1. Overview of TTX & Drills
2. Examples / Past Experience

Resilience and Preparedness

- Outcome of Incident Response planning
- Prepare - Understand risks, exposure
- Develop – process, capabilities, point of contacts
- Practice - Respond and minimize impact of security incidents
- Recover (quickly)

Realities

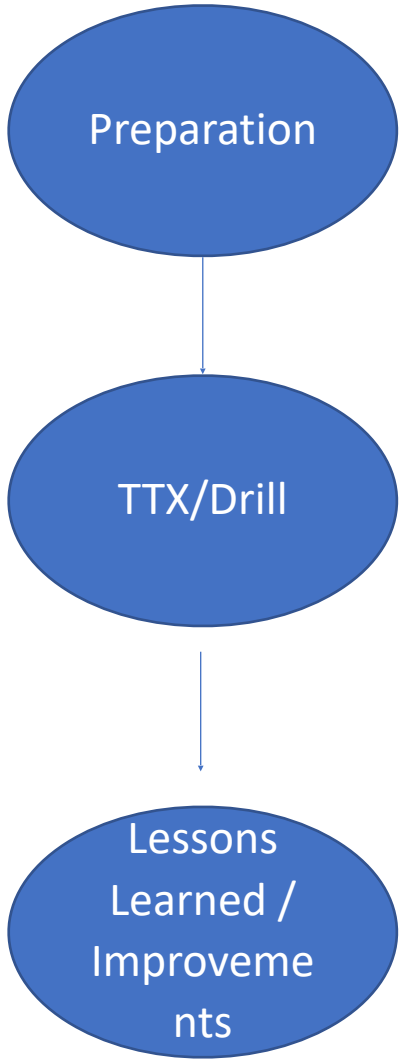
- Cyber Security practice and capabilities of organisations are different
- People leave organisations (with knowledge & expertise)
- Incidents and Breaches happens
- Incident Response involves everyone in the Organisation (and Eco-System i.e. National Level)
- Learning through real incident can be costly

TTX and Drills

- What if that happens to us?
  - Our current state
- Focus on different aspects of Incident Response
  - Education/Awareness, Technical, Communication, Decision Making, Process
  - Improvement of Incident Response – identify gaps
- Work on a scenario or Multiple Scenarios
- Facilitation - someone with incident response background
- Table Top Exercise – walkthrough, discussion based
- Cyber Drills – more hands-on, infrastructure, artifacts (logs, malware, systems)
  - “Cyber Range”

TTX & Drills (2)

- Can be carried out at
  - Organisational, Sectoral, National, Regional, Global level
- Not a competition (like CTF)
  - Guided – move to the right direction
  - Reflect on gaps and capabilities, potential improvements & learning
- Can be more effective than talking/teaching concepts or ideas
- Supplements – policies & procedures



Examples

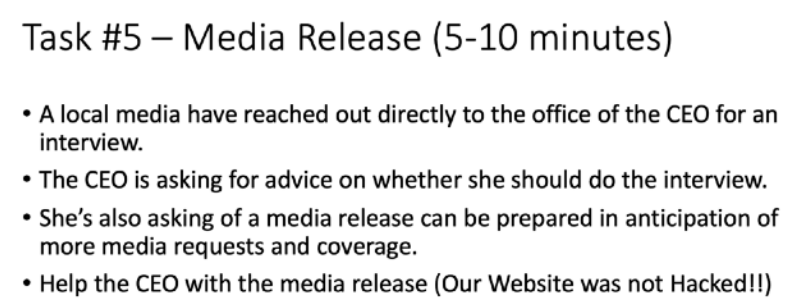
Data Breach (TTX)

- Scenario: Data Breach with attacker engaging with the organization on social media. Initial ransom request escalates into publication
- Duration (90 – 120 minutes)
- Objective – awareness & education of incidents & incident response
- How – discussion to focus on response of (1) Management (2) Legal (3) Communications (4) IT
- Discuss best practices, internal reflection and answer questions from the audience. Focus on decisions and time frame

DNS Hijacking TTX

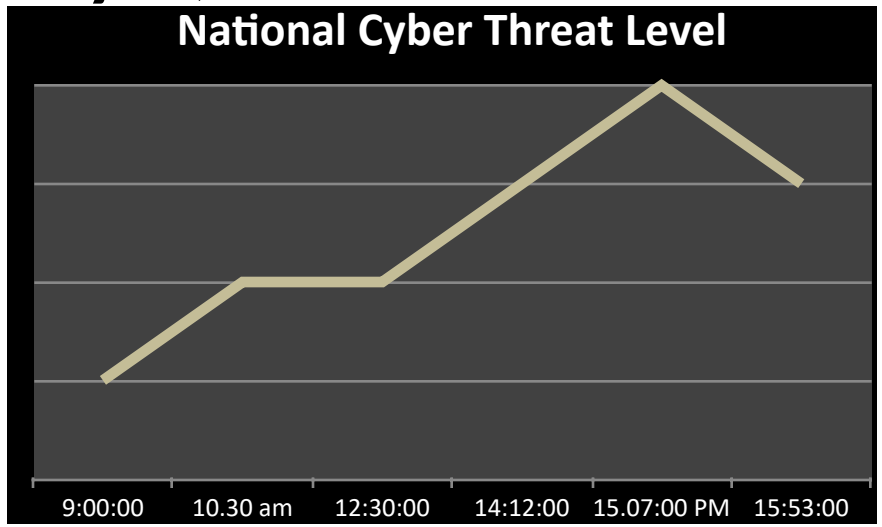
- Scenario:
  - DNS Hijack of A records & MX (Mail Exchange)
  - Incident visible to public, affect business
  - Potential Personal Information Breach
- Duration: 120 minutes++
- Focus
  - Communication aspect of the incident
  - Internal communication, social media, media release, interview, Advisory, request for assistance and reporting to authority/regulatory
- How
  - Give task to produce communication outputs based on development of the incident
- Discuss communications best practice, templates, being transparent & controlling narratives

https://www.dragonfly.air

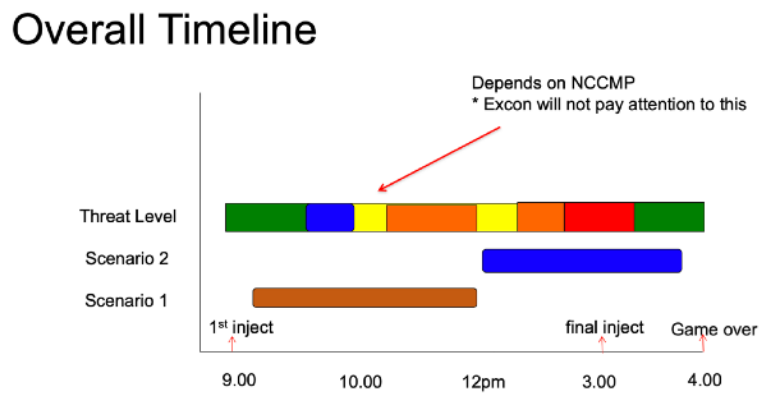


Task #5 – Media Release (5-10 minutes)

Annual National Cyber Drill (X-Maya)

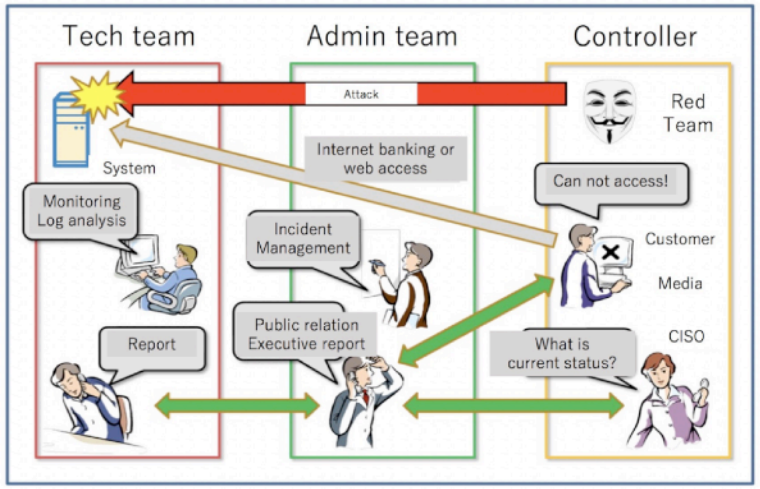


- Scenario: Multiple (botnets, ddos, APT, etc)
- Duration: ½ day – 1 full day + debriefing session
- Focus:
  - Critical Infrastructure Agencies (more than 100 orgs)
  - National Crisis Management Plan
  - Technical, Process, Information Sharing and Understanding Eco-System
- Preparation
  - dedicated team, a few months of prep, pre-drill workshops
  - Need $$$
- How – Every organization work on scenarios & respond to co-ordination by central agencies
- Discuss observations, compare notes, improvements in debriefings, expectations
- Scalability challenges in the long run



CyberQuest – (FS-ISAC Japan)

- Scenarios: Financial Sector related incident (phishing, banking trojan, etc)
- Duration: 1 full day + debriefing
- Focus: Collaboration, Incident Response (technical and management/CISO) including recovery
- How :
  - 2 teams with technical and management representatives from different banks
  - Separate infrastructure for each team to deal with live incident
  - Press Conference by CISO and management
- Discuss on best practices and action taken by both teams
- https://blog.apnic.net/2017/02/06/cyberquest-incident-handling-exercise-japanese-financial-industry/



APCERT Annual Drill (2007)

- Scenario: Beijing Olympics 2008 with multiple incidents
- Duration: ½ day
- Focus: Collaboration, Communication and technical aspect of attacks i.e. ddos and botnets
- How:
  - Participants were National CERTs & members of APCERT
  - Scenario developed so that CERTs will contact one another and share intelligence
  - Scenarios were also flexible so that national certs can extend the drill locally (with ISPS or other agencies)
- For regional or Global drills – using an upcoming event (sports, meetings) can be useful
  - i.e. Pacific Games 2019 for Pacific Island region CERTs in 2018

- **0700** Lord of Armageddon (LoA) declare cyber war on Beijing Olympics
- **0900** Co-ordinated botnet attacks from AP region causing media sites and government portals inaccessible
- **1100** Spam containing malware that turns PC into zombies were filling up mailboxes in AP economies
- **1300** Border and Core routers crashing and rebooting frequently. 0-day exploit for Cisco IOS rumoured to be available. Cisco promise to release fix in a few hours
- **1430** – Cisco released patch and advisory on critical IOS vulnerability
- **1600** – Security analysts announced that bots automagically removed themselves, no more attacks

Conclusion

- Table Top Exercise and Drills can help improve incident response preparedness
- It allows you to focus on an area or some areas of incident response
- It helps everyone to be on the same page
- It is critical to follow up on the gaps with improvements
- Resources will be required depending on the size and complexity
- Free Resources available (i.e. FIRST Breach Workshop)

Resources

- https://www.first.org/education/trainings#Breach-Workshops
- https://blog.apnic.net/2017/02/06/cyberquest-incident-handling-exercise-japanese-financial-industry/

Thank you

- Adli Wahid
  adli@apnic.net

  www.apnic.net