27th ANNUAL

FIRST CONFERENCE BERLIN

14-19 JUNE 2015

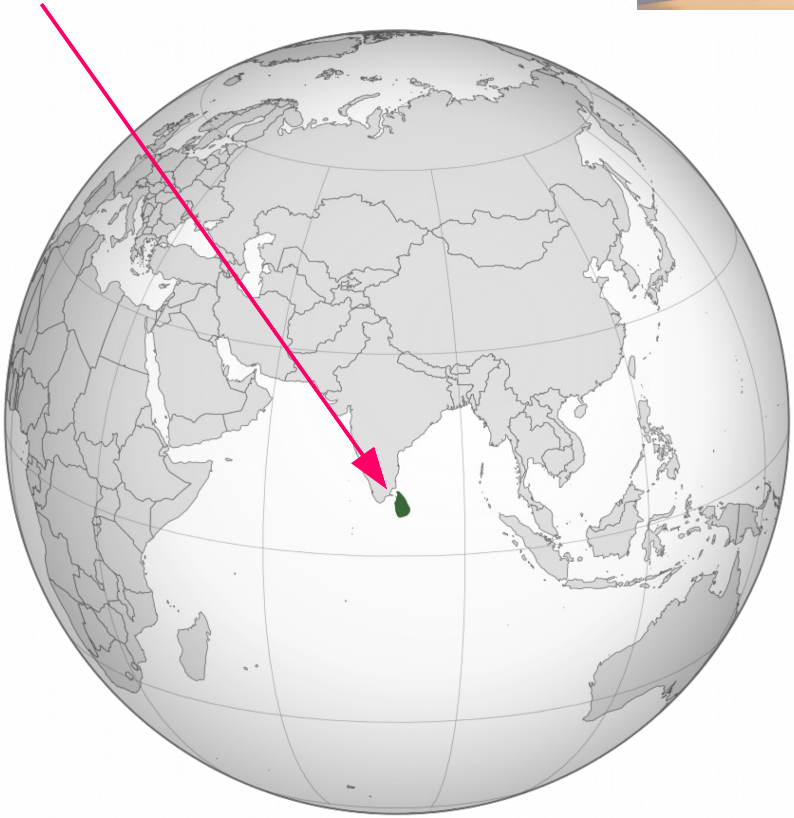
UNIFIED SECURITY: IMPROVING THE FUTURE

Sector Based Cyber Security Drills Lessons Learnt

Dileepa Lathsara

TechCERT Sri Lanka

Sri Lanka



Population : ~20 Million
Area : 65,610 KM^2
Capital: Colombo
TLD: .lk

TechCERT

Background:

- Collaborative effort of TechCERT and COMPUTER SCIENCE & ENGINEERING UNIVERSITY OF MORATUWA
- SINCE 2011
- Initially introduced to the ***banking sector***

  then… → *financial* → *insurance* → *Telco sector*

- Idea and the experience gained from APCERT Annual Drill

The main objective of the cyber drill exercise

- Train IT and IT Security staff to successfully overcome a cyber-attack
- Evaluate the security team’s response to cyber-attacks.
- Check the contingencies of their IT processes and procedures
- Test technical competency in dealing with cyber attacks
- Realization of overall attack and how they handle the situation
- Test the communication contact points and **internal team communication**
- How they successfully **communicate with the media** without affecting confidentiality
- Encourage Coordination and **information sharing** between trusted parties/stakeholders and competitors to mitigate the attack

TechCERT Cyber Security Drill

TechCERT

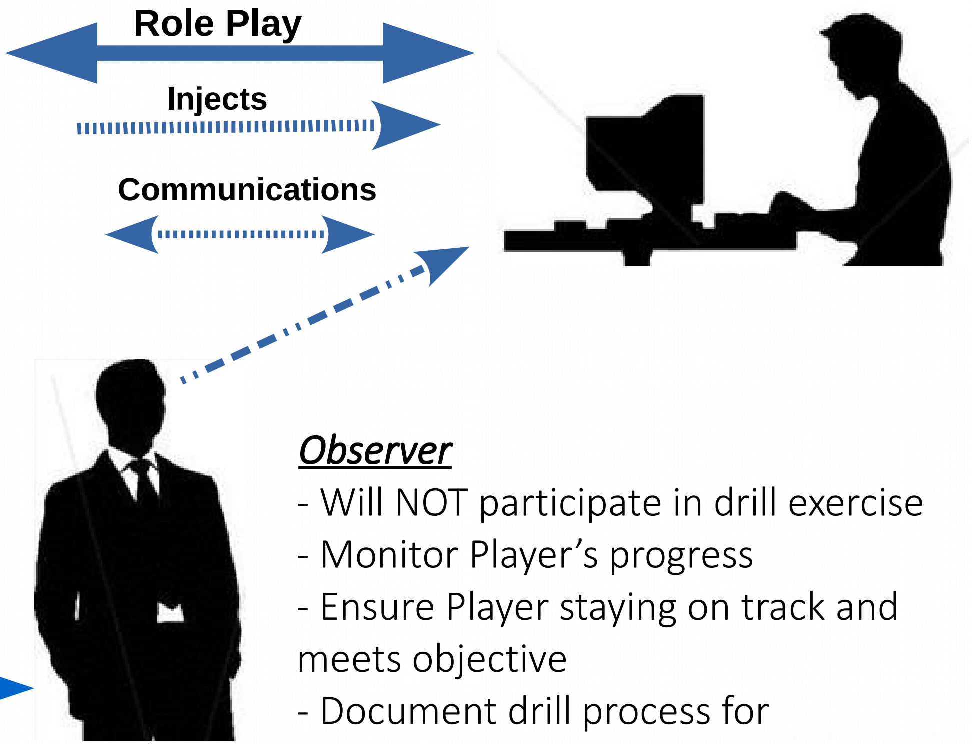
Roles in the Drill

Drill – Exercise Control (D-CON)

- Declare start/end of drill
- Send out injects to Players
- Respond to Player responses by acting as different parties (i.e ISP, Attacker, Customer, Media, CEO, IT Team)
- Control the progress of drill

Player

- Staff of participant organization who respond to security incidents
- Should react to the given ‘Injects’ as in daily operations



Role Play

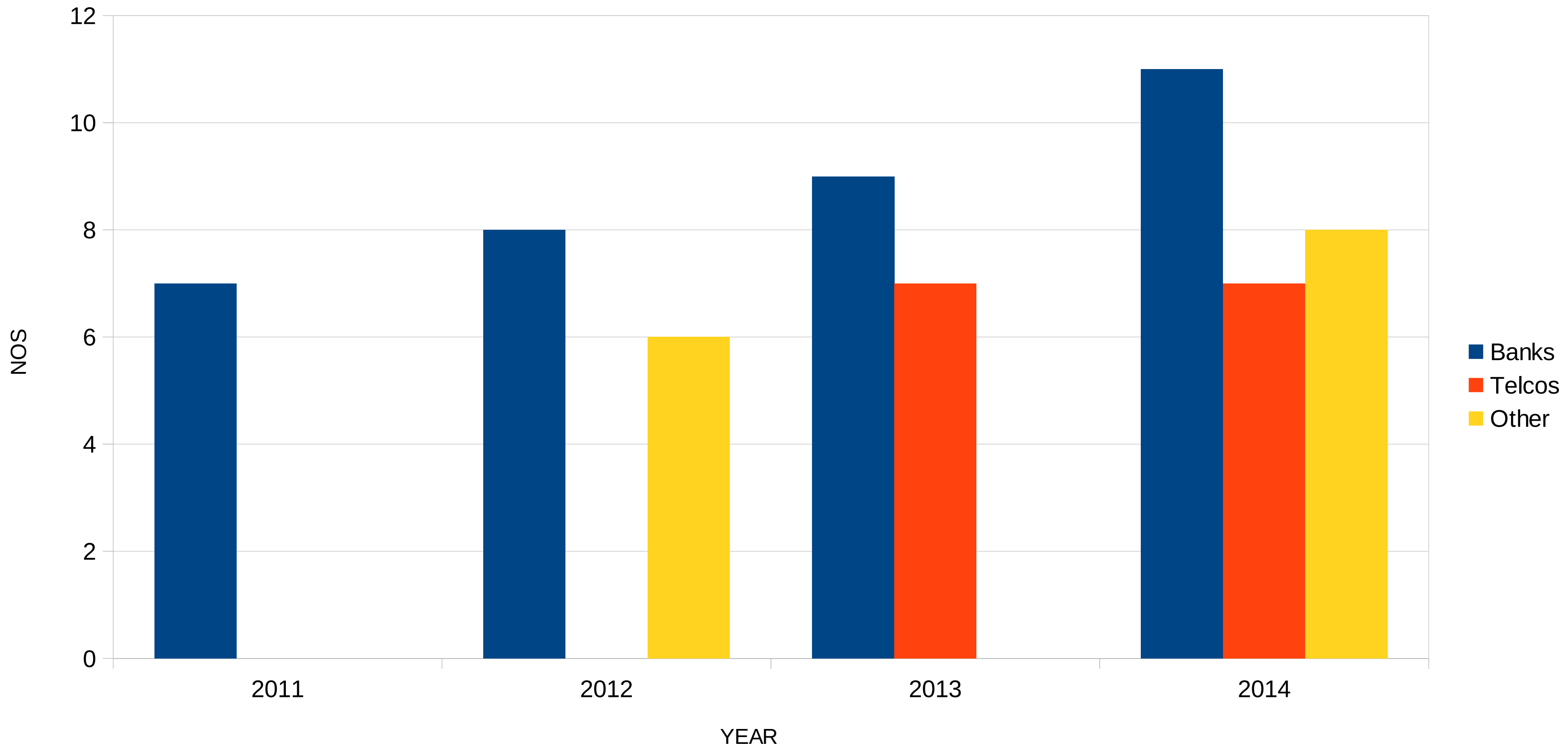
Injects

Communications

Observer

- Will NOT participate in drill exercise
- Monitor Player’s progress
- Ensure Player staying on track and meets objective
- Document drill process for evaluation

Progress of TechCERT Cyber Security Drills



Progress of TechCERT Cyber Security Drills

Year	Theme	Number of organizations		
		Banks	Telcos	Other
2011	Advanced phishing attack	7	-	-
2012	Advanced persistent threats and coordination	8	-	6
2013	Countering Large Scale Denial of Service Attacks and Coordination	9	7	-
2014	Strength of a Chain Lies on Weakest Link	11	7	8
2015	Free doesn’t necessarily mean free	July 2015	August 2015	7

Some lessons cant be taught
They simply have to be learned

Jodi Picault

Deciding a theme

Problems Encountered:	Lessons Learnt
• Conducting a drill based on the proposed theme	• Possibility of conducting a drill based on the proposed theme needs to be evaluated before the final decision • Drills should follow current happenings in the cyber security arena

Deciding the Drill scenarios/Injects

Problems Encountered:	Lessons Learnt
• Participants are unable to identify the incidents clearly • Realization of overall attack is difficult / not clear	• Allowing some of the D-CON team members who did not participate in the design to go through all the drill scenarios / injects before the final preparation. • Joint brainstorming sessions • Sending drill objectives to "Observers"

Drill communication

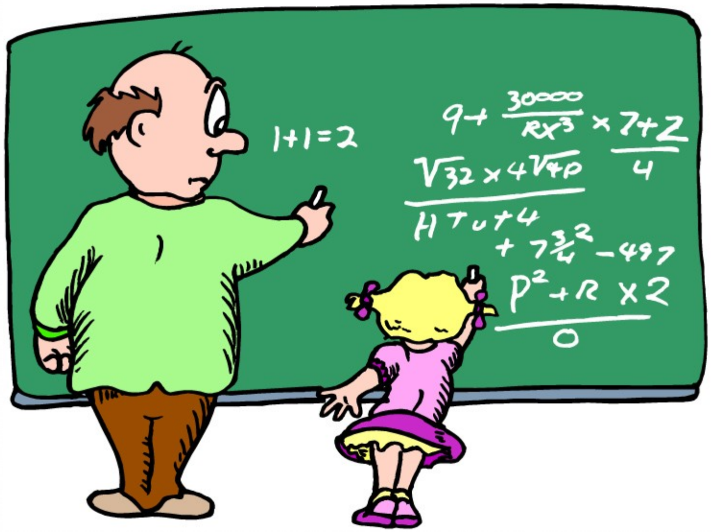
Problems Encountered:	Lessons Learnt
• Not familiar with responses expected during the drill • Infrastructure was not prepared in the drill time • Participating teams were not serious	• Pre-drill communication test. • All the communication mechanisms need to be tested before • Questionnaire should be designed to ascertain whether the participants are thorough with the guidelines provided during the registration process

The Drill Day

Problems Encountered:	Lessons Learnt
• In reality, time spent on certain incidents is much longer	• Some parts of the actual incident details needs to be communicated at least one or two hours prior to the drill • Observers ensure that players stay on track and meets objectives

Participating team capabilities are different

Problems Encountered:	Lessons Learnt
• Some participating teams are fast and accurate while other teams struggle to complete the tasks. • Maintain the same intensity of enthusiasm entire time.	• Analyze the responses of the relevant teams for the last drill. • Maintain different injects / threat information depending on the team's capability. • Keep TechCERT team members on site and guide the teams if necessary



TechCERT

Drill and daily operations

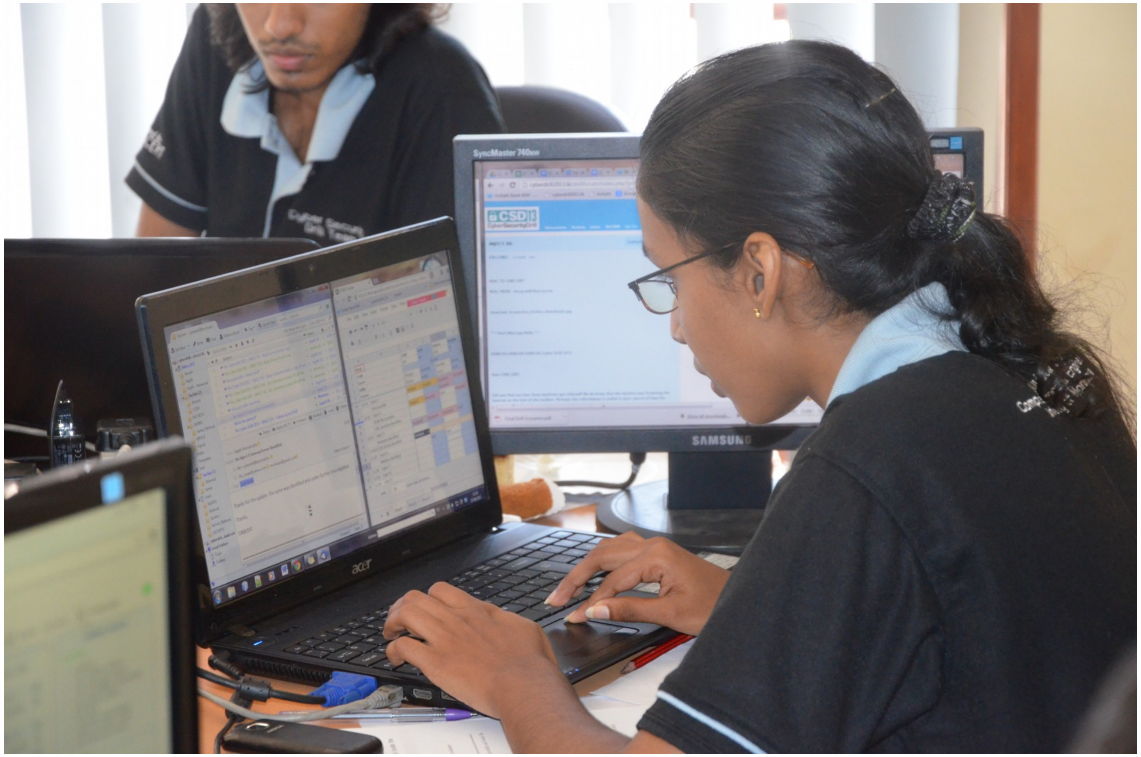
Problems Encountered:	Lessons Learnt
• Some teams were unable to cope with their day-to-day tasks	• Drill should be designed so that teams’ normal activities should be carried out undisturbed. • Sending specific instructions at least a week prior to commencement of the exercise should result in participating teams being ready well ahead of the exercise date.

Malware Analysis

Problems Encountered:	**Lessons Learnt**
• Malware analysis/log analysis and similar activities take a lot of time	• Conduct more activities related to malware/log analysis, DF investigations. • Train and provide them the necessary tools • The following will be evaluated during such activities: - Whether the team is able to react - How fast a team can react - How accurate the results are

Resource limitations

Problems Encountered:	Lessons Learnt
• Manpower requirement to conduct national level drills	• Get help from university students (Engineering undergraduates) after training them.



Evaluation report and team performance

Problems Encountered:	Lessons Learnt
• Should not be shared with external parties.	• Drills should not be considered as a competition. • The teams’ performances should not be shared with other teams, as doing otherwise will affect the continuation of the drill. • But presentation to the Management is a must

Conclusion and Recommendations

- Organizations have realized that they depend a great deal on external partners and organizations (Service providers, ISPs, CERTs).
- Acquiring up-to-date knowledge is very important for all personnel handling information security issues. (Trainings, Certifications)
- IT security teams should build trusted relationships with relevant stakeholders, including their competitors.

Conclusion and Recommendations

- Many organizations had taken steps to update their incident response strategies based on the evaluation report given.
- Sector-based cyber security drill set the stage for all the Sri Lankan organizations to secure their vital information from cyber-attacks and took a lead role in securing Sri Lanka's cyberspace.

TechCERT

HELPING YOU SECURE YOUR INFORMATION ASSETS

lathsara@techcert.lk
www.techcert.lk