27th ANNUAL
FIRST CONFERENCE
BERLIN
14-19 JUNE 2015

UNIFIED SECURITY:
IMPROVING THE FUTURE

27th ANNUAL FIRST CONFERENCE BERLIN 14-19 JUNE 2015

Sector Based Cyber Security Drills Lessons Learnt

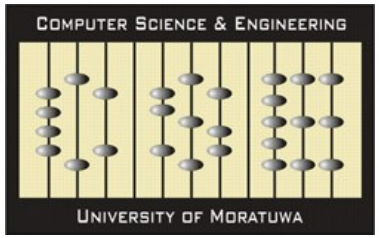
Dileepa Lathsara

TechCERT

Background:

- In the past five years, cyber-attacks and threats on corporate IT systems in Sri Lanka is in the rise.
- Many organizations start reacting to security incidents after the fact.
- Organizations are lacking experience and expertise to successfully over come Cyber attacks.

Background:

- Collaborative effort of TechCERT and 

- SINCE 2011
- Initially introduced to the ***banking sector***

  then… ➡ *financial* ➡ *insurance* ➡ *Telco sector*

- The attack scenarios for the drill will be based on the latest cyber-attacks
- 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

The main objective of the cyber drill exercise

- 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 to mitigate the attack

About TechCERT Cyber Security Drill

- Simulate scenarios for pre-defined objectives,
- Providing necessary stress to players - react to an untold situation within a time limit.
- Role-playing game between the Players and the Drill Control Center D-CON.
- Supplies the ‘injects’ according to the predefined timing
- Simulated scenario is made as close to reality as possible within safe boundaries
- All information may not be given explicitly. Some may require the player to dig out

Sample Drill Scenario

Sample Drill Scenario

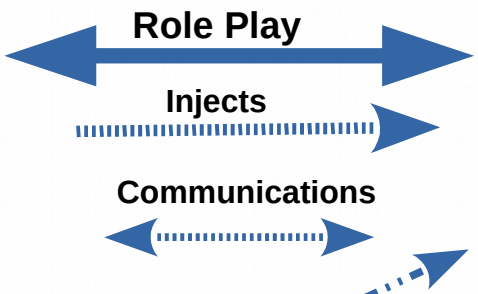
Roles in the Drill

Drill – Exercise Control

- 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)

Player

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



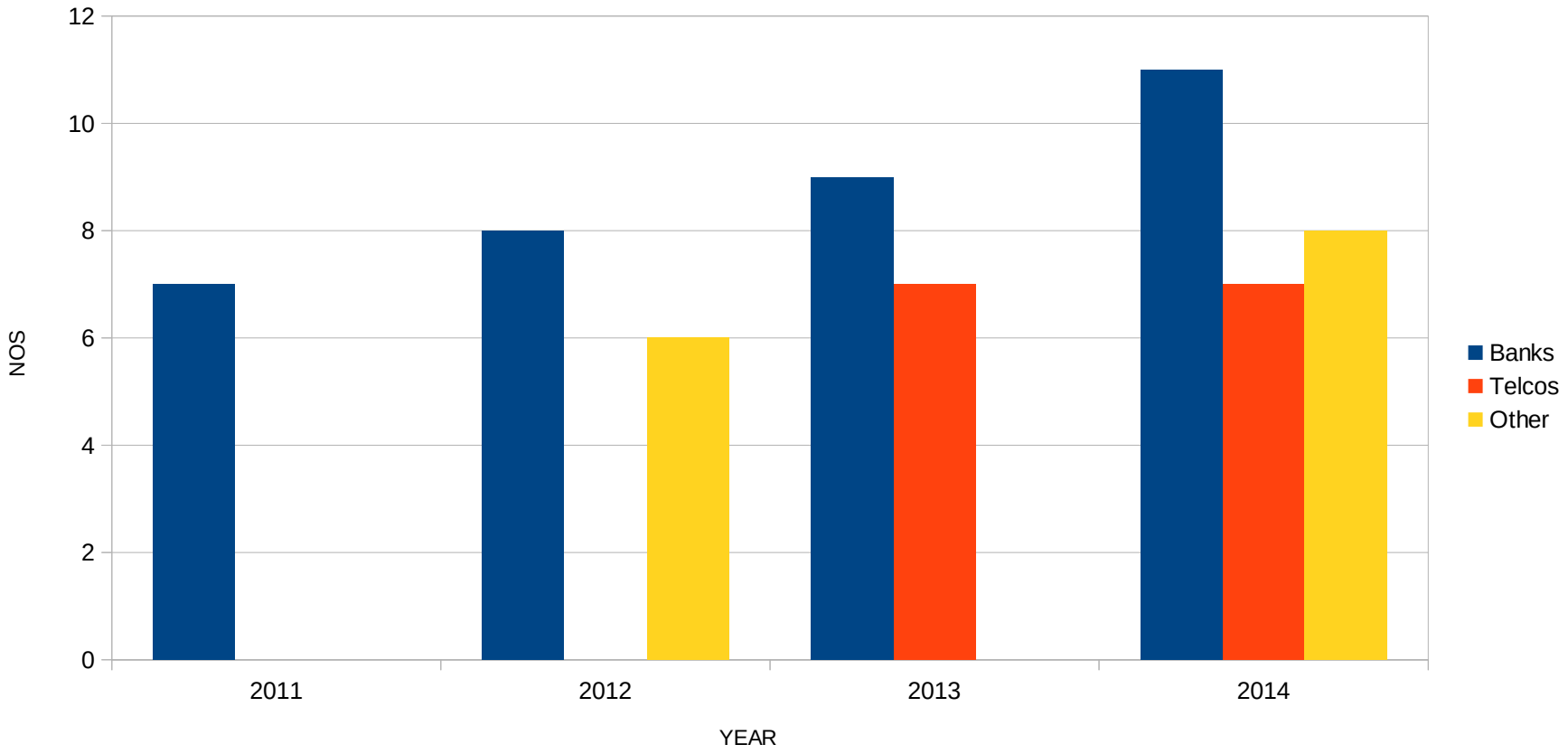
Observer

- 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

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 safe	July 2015	August 2015	7

Progress of TechCERT Cyber Security Drills



Some lessons cant be taught
They simply have to be learned

Jodi Picault

Description	Problems Encountered:	Lessons Learnt
Decide a theme		• Drills should follow current happenings in the cyber security arena • Possibility of conducting a drill based on the proposed theme needs to be evaluated before the final decision
Deciding the Drill scenarios/Injects	• Participants (Players) 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 to prepare the high-level drill scenario with all D-CON members • Sending drill objectives to “Observers” of the participation teams

Description	Problems Encountered:	Lessons Learnt
Drill communication	• Participants were not familiar with responses expected during the drill • Some teams' infrastructure was not prepared in the drill time • Some of the participating teams were not serious	• Pre-drill communication test should be a complete rehearsal of the drill • All the communication mechanisms need to be tested beforehand • Questionnaire should be designed to ascertain whether the participants are thorough with the guidelines provided during the registration process
The Drill Day	• In reality, time spent on certain incidents is much longer • Some of the teams were unable to cope with the elements being exercised	• Some parts of the actual incident needs to be communicated at least one or two hours prior to the drill • Observers ensure that players stay on track and meets objectives • Keep TechCERT team members on site

Description	Problems Encountered:	Lessons Learnt
Drill and daily operations	• 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	• Malware analysis/log analysis and similar activities take a lot of time • Teams need to improve their capabilities in this regard.	• 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

Description	Problems Encountered:	Lessons Learnt
Team capabilities are different from sector to sector	• Response to the incidents of some participating teams are fast and accurate while other teams struggle to complete the tasks • Maintain the same intensity of enthusiasm during the entire drill	• Analyze the responses of the relevant teams for the last drill. • Maintain different injects / threat information depending on the team's capability.
Resource limitations	• Manpower requirement to conduct national level drills	• Get help from university students (Engineering undergraduates) after training them.
Evaluation report and team performance	• 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

- They have realized that they depend a great deal on external partners and organizations (Service providers, ISPs, CERTs) when it comes to cyber-attacks.
- Acquiring up-to-date knowledge is very important for all personnel handling information security issues. Therefore, advanced security training for IS team members and basic security training for all IT team members is a must for all sectors.
- Cooperation is very important in successfully handling cyber-attacks. Therefore, all IT security teams should build trusted relationships with relevant stakeholders, including their competitors.

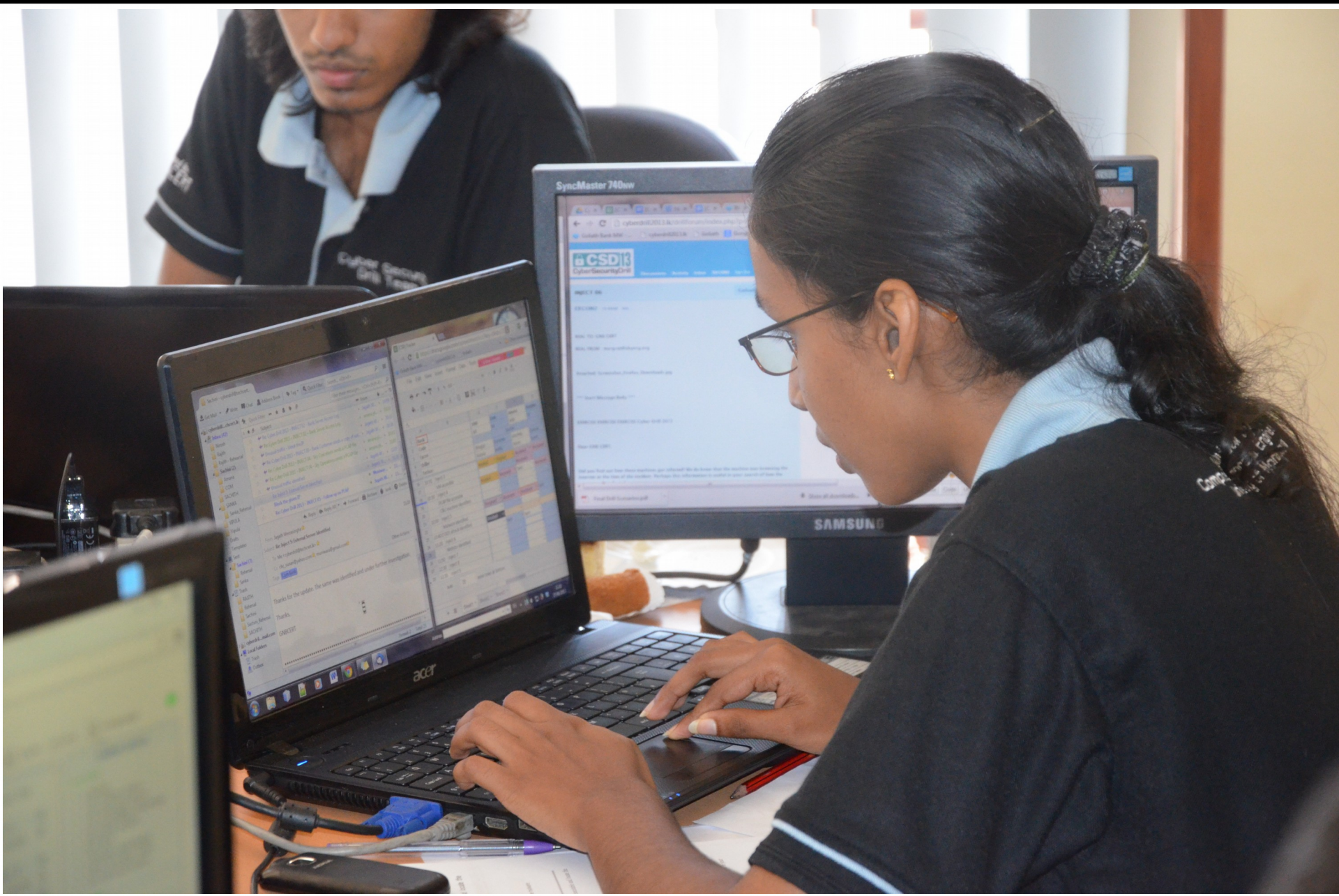
Conclusion and Recommendations

- Feedback shows that all teams stood to benefit by the drill. 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 the banking, finance, telco, ISP, insurance, and other participating teams from several sectors 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


SyncMaster 740nw
SAMSUNG
acer