RSA Conference 2016

Learning Labs

Financial Sector and the Evolving Threat Landscape: Live Cyber Exercise

Post-Conference Summary

Speakers:

- **Kevin Jonkers, Manager Forensics & Incident Response**
- **Krijn de Mik, Principal Cyber Security Expert**
- **Sarah Brown, Principal Cyber Security Expert**

Table of Contents

RSA Learning Labs

Introduction

Fox-IT developed a financial cyber crisis table top exercise for the Learning Labs portion of the 2016 RSA Conference. This was designed as a paper-based exercise with a facilitated discussion of a scripted scenario, where planners and players sit together in one room for the exercise execution.

The intent of the exercise was to:

- elicit constructive discussion as participants examine and resolve problems
- identify where existing approaches need to be refined
- establish relationships and share information with other organizations, partners, and countries
- raise the awareness of the security community about challenges when dealing with a financial sector cyber crisis

The exercise provide an opportunity to address a cyber threat scenario in an interactive and collaborative tabletop exercise. It examined challenges and best practices for a range of personas who handle cyber threats—C-suite, law enforcement, SOC, threat and incident analysts—exercising the ability to respond to a rapidly emerging and growing financial sector threat. The events were hypothetical, pre-planned, and documented.

Exercise Format and Logistics

The exercise took two hours to complete. The room was divided into five teams of ten (10) people. Each team role played a crisis team made up of a range of personas who handle cyber threats—C-suite, law enforcement, SOC, threat and incident analysts.

There were (3) facilitators during the exercise, who presented each update and discussed the progress of the teams, and answered any questions that arose from the teams.

The Teams

After the teams were assembled, roles were picked for the crisis team. The participant could choose the roles of amongst others CIO, CISO, HR Director, PR Director, General Counsel, and IT director.

If more people were attending a team than there were roles, the participant were free to appoint multiple people to the role. Once assigned, the job was to make sure that the department's interests were presented throughout the crisis.

Fortunately, many of the roles were represented by players who had these roles in real life during the event at RSA.

How We Played

As the crisis unfolded, updates were given and the teams had time to discuss the actions that their members took. There were 6 short rounds.

Updated information on the unfolding crisis was presented, and teams were asked to submit their responses via the Exercise Scoreboard on their tablet.

We played according to the following schedule:

- Introduction of new information (3 mins)
- Discussion within team (10 mins)
    - Define priorities
    - Define top 3 next steps
    - Enter both on the tablet
- Evaluate responses from the teams (3 mins)

After each round, (virtual) time was fast forwarded and new information was presented for the next round.

Priorities

The participants were asked to score (1-10) the following priorities during every round:

- Restore operations
- Avoid regulator/auditor scrutiny
- Prevent/restore reputational damage
- Avoid/influence media coverage
- Minimize customer impact
- Minimize direct incident costs
- Identify root cause
- Identify adversaries

The closer the team was to Fox-IT's score, the more points they received.

Setting the Scene

Goliath National Bank (GNB) is a prominent retail bank, offering financial products to both companies and individuals in the country of Ramul, a (fictitious) European democracy. GNB provides the following products to its customers:

- retail
- direct
- private
- investment
- commercial banking
- insurance
- asset management

The history of the bank goes back to 1817 when the first Ramulian savings bank was established. The savings bank movement was part of a campaign to encourage individual citizens to save for their future.

According to the Fortune Global 500, in 2015 Goliath National Bank was Ramul's largest bank and insurance conglomerate and the largest bank in the country, with a workforce of 10,000. GNB is a key part of Ramul's national critical infrastructure.

GNB is part of the Goliath Banking Group, based in Hong Kong. The bank trades on the Hong Kong Stock Exchange.

Ramul enjoys a strong economy and first-world status as a nation. It is a prosperous nation. Across the world at this time, a political risk report, geopolitical tensions between the East and West are on the rise lately because of:

- Falling oil prices
- Europe's recent sanctions on the (fictitious) nation of Kamon
- Political violence in unstable regions of the world

The report recommends strategies for managing political risks and also looks beyond the next couple of years to consider 2017, when elections in several countries could significantly alter the political risk landscape.

The participants of this Learning Lab were told they were longtime employees of GNB, enjoying another nice day at the office when the phone rings… the Learning Lab participants were asked to meet downstairs for an impromptu meeting requiring their immediate attention.

Conclusions & lessons learned

- As crisis teams work through serious events, there is often partial information, unclear causes of events, and unclear future effects. Therefore, war gaming and cyber crisis table top sessions are required on a regular basis for the crisis management team to gain experience in this field of expertise.
- At each point during the crisis, organizations must decide where to focus their attention and resources based on the stakeholders involved in a particular phase of the crisis:
  - Restore operations
  - Avoid regulator/auditor scrutiny
  - Prevent/restore reputational damage
  - Avoid/influence media coverage
  - Minimize customer impact
  - Minimize direct incident costs
  - Identify root cause
  - Identify adversaries
- A crisis team needs a decision framework and playbooks they can use to solve the crisis in an efficient and effective manner. The framework should accommodate the team in making decisions about the priorities that are important at a specific moment in time, but also when the

organization has to disclose information and to which stakeholders. Not having processes in place to ensure timely and consistent communication with stakeholders can lead to damaging consequences. Bad communications can contribute to overall confusion about the situation among key audiences, initiate rumors, and trigger a selloff of company's shares[1].

- Crisis teams require input from HR, PR, Legal, IT, and the CISO (at a minimum) to address the potential issues that can arise from a crisis.
- The most difficult phase of the Learning Lab (as well as in a real life incident) is the moment a crisis team receives the details about how the incident took place. From that moment in time the team has to switch from focusing on 'identifying the root cause' to 'restoring operations'. They must find a healthy balance wherein the investigation continues, but the 'restore operations' priority becomes the most important. We can call this moment between investigation and mitigation an 'impasse moment'. In order to make the right call, the crisis management team should be able to look at the incident from a helicopter view and come to a clear decision with regards to the next steps, by taking into account the investigation findings, business interests and potential future consequences related to the incident.

For more information

Feel free to contact us in case you would like to receive more information related to the table top session. You can call the phone number below and the office management will forward your call to Kevin Jonkers, Krijn de Mik, or Sarah Brown:

- +31 (0)15 284 79 99

[1] http://www.sciencedirect.com/science/article/pii/0007681385900357.