ROOM #42
How to face a cyber crisis?

Feedback and toolbox
1. PRESENTATION
2. BASIC ELEMENTS
3. OBJECTIVES
4. PROCESS
5. FEEDBACK
6. SIMULATION
7. KEY POINTS
8. SUMMARY
9. TIPS

ROOM#42 OBJECTIVES

TRAIN BY DOING

LEARN REFLEX ACTION

IMPROVE MATURITY LEVEL
1. PRESENTATION
2. BASIC ELEMENTS
3. OBJECTIVES
4. PROCESS
5. FEEDBACK
6. SIMULATION
7. KEY POINTS
8. SUMMARY
9. TIPS
CRISIS MANAGEMENT

1. PRESENTATION
2. BASIC ELEMENTS
3. OBJECTIVES
4. PROCESS
5. FEEDBACK
6. SIMULATION
7. KEY POINTS
8. SUMMARY
9. TIPS
• Around 100 exercises
• 2,5 years of existence and operation
• Sectors concerned: public sector, media, insurance, banks and various organisations
<table>
<thead>
<tr>
<th>Attack / Incident</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto-ransomware</td>
<td>- 85 % of participants need more than 15 minutes to react</td>
</tr>
<tr>
<td></td>
<td>- 60 % of countermeasures are insufficient</td>
</tr>
<tr>
<td>Fake news</td>
<td>- 65 % of participants do not clearly reject the press release</td>
</tr>
<tr>
<td>Defacing</td>
<td>- 35 % of participants don't know what to do</td>
</tr>
<tr>
<td>Social engineering</td>
<td>- 10 % of participants give a password by phone to a stranger</td>
</tr>
<tr>
<td>Cybercriminals</td>
<td>- 40% of the participants pay the ransom</td>
</tr>
<tr>
<td>Crisis</td>
<td>- 45 % have never activated the crisis team</td>
</tr>
<tr>
<td>CERT</td>
<td>- 70 % of participants do not seek help from a CERT</td>
</tr>
<tr>
<td>Communication</td>
<td>- 80 % of participants forget to communicate internally</td>
</tr>
<tr>
<td>Forensic</td>
<td>- 95 % don't think about collecting logs and evidence</td>
</tr>
</tbody>
</table>
Point 1: Trigger of the "crisis"

-> How do I know that I am in a "crisis"?

The 4 key questions to determine your state of crisis:

- Are we facing an unforeseen event?

- Is there an urgency in the decision-making?

- Are we facing an event that threatens the company, its survival, and its external environment?

- Who will manage the crisis (Cyber Response Team -> In the event of a cyber crisis)?
Feedback from point 1

What we see:

**Problem with the human factor:**
- Fear to launch the crisis management procedure
- Difficulty to create a crisis management team:
  - 1 decision maker
  - 1 communicator
  - 1 risk manager
  - 1 IT manager
Point 2: The cape!

-> 3 key questions to make an effective situation update

Where am I?
- Assessment of the situation

Where do I want to go?
- My objective

How can I get there?
- My means
Feedback from point 2

- Waste of time with non-essential questions and concerns
- Lack of simplicity
- Lack of coordination
- Difficulty making decisions
Point 3: Determine the objective of crisis management

What is the **purpose of a crisis management plan?**

- Limit the impact(s)
- Limit the deterioration of the situation
- Prevent disaster
Feedback from point 3

Several errors are often made at this level:

- React lately
- Underestimate impacts
- Lack of internal communication
- No crisis strategy

Consequences noted:

- Waste of time
- Precipitation and wrong decisions from the start
Point 4: The timeline

This point is essential to list all events and incidents impacting us!
Feedback from point 4

In 90% of cases, no timeline is performed!

How?

Create a simple Excel table and indicate:
- Event or incident number
- Date and time of reporting
- Describe the event / incident detected
- Person who detected
- Action already taken

<table>
<thead>
<tr>
<th>No.</th>
<th>Incident or Event</th>
<th>Date</th>
<th>Time</th>
<th>Who detected/touched</th>
<th>Action already taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A virus has contaminated an employee laptop</td>
<td>04/15/2020</td>
<td>16:45</td>
<td>James LABORDE</td>
<td>Laptop isolated</td>
</tr>
<tr>
<td>2</td>
<td>The web site of the company is defaced</td>
<td>04/16/2020</td>
<td>01:34</td>
<td>Sophia CASTEL</td>
<td>Server stopped</td>
</tr>
<tr>
<td>3</td>
<td>The mailbox of the communication manager is compromised</td>
<td>04/16/2020</td>
<td>06:45</td>
<td>Pierre DUPONT</td>
<td>Password changed</td>
</tr>
<tr>
<td>4</td>
<td>10% of the client list leaked</td>
<td>04/16/2020</td>
<td>09:24</td>
<td>Emma STONE</td>
<td></td>
</tr>
</tbody>
</table>
Point 5: Measure the impacts

Measuring an impact is:
- Understand it
- Determine the processing priority

Classify impacts:
- Financial: How much will I lose / cost?
- Reputation: Who is informed?
- Legal: What is the risk?
- Operational: What is no longer working?
Feedback from point 5

Two cases regularly observed:

- Impact analysis is not performed
- Impact analysis is neglected
Point 6: Create an action plan

It must indicate the following information:

- **Action by priority** (estimated beforehand at impact level)
- **Expected effect/benefit**
- **Cost**
- **Person responsible for the application**
- **Implementation deadline**

<table>
<thead>
<tr>
<th>N°</th>
<th>Incident or Event by priority</th>
<th>Actions</th>
<th>Cost</th>
<th>Responsible</th>
<th>Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/10</td>
<td>the client list was leaked</td>
<td>1. Contact lawyers 2. Contact Police 3. Contact CNPD and CSSF 4. Contact clients impacted ... 5. Write a press release 6...</td>
<td>1 000 000 euros</td>
<td>Steve BONHO</td>
<td>04/22/2020</td>
</tr>
<tr>
<td>2</td>
<td>The website of the company is defaced</td>
<td>5. Restore the last version of the website 2. Change password of the web server 3. Update OS of the web server 4. Analyse logs</td>
<td>NA</td>
<td>Pierre ETIENNE</td>
<td>04/16/2020</td>
</tr>
<tr>
<td>3</td>
<td>The mailbox of the communications manager is compromised</td>
<td>2. Change all mailbox passwords 1...</td>
<td>NA</td>
<td>Mélanie RIOUX</td>
<td>04/16/2020</td>
</tr>
<tr>
<td>1A</td>
<td>A virus has contaminated an employee laptop</td>
<td>3. Change laptop 2...</td>
<td>NA</td>
<td>Olivier LOYS</td>
<td>04/17/2020</td>
</tr>
</tbody>
</table>
Feedback from point 6

The actions plan is often non-existent.
Point 7: Stay cyber vigilant

Chaos comes with chaos!

Chaos is the best place for cybercriminals

They will use this situation to:

- Destroy
- Financial gain
Often the crisis committee drops its guard once the action plan has been drawn up and put into practice.

-> Error!!!

Never forget Murphy's Law!
Point 8: Time for action!

- **Apply the first measures** of the actions plan
  - Organizational
  - Communication
  - Technical
  - Human
  - Legal
  - …

- **Measure their effectiveness**

  Detail: If you are attacked -> **Remember to keep the evidence!!!**
An extra **effort on the technical** points is often noted to the detriment of the **human and communication** aspects...

**Knowing how to communicate:**

- Give **simple instructions** to staff
- **Reassure customers**
- **Inform the media**
- **Stay connected with partners**
- **Exchange information** with "allies"
Point 9: Getting out of the crisis

Normally, the end of the crisis occurs when:

- The measures in response to the crisis were:
  - Applied
  - Efficient

- Activity resumes to normality

- Be able to say: “The crisis is over!”

This remains the most complex decision to make.
CRISIS MANAGEMENT

1. PRESENTATION
2. BASIC ELEMENTS
3. OBJECTIVES
4. PROCESS
5. FEEDBACK
6. SIMULATION
7. KEY POINTS
8. SUMMARY
9. TIPS
Tip 1: Be cyber vigilant
Tip 1: Be cyber vigilant

Tip 2: Make simple decisions
1. PRESENTATION
2. BASIC ELEMENTS
3. OBJECTIVES
4. PROCESS
5. FEEDBACK
6. SIMULATION
7. KEY POINTS
8. SUMMARY
9. TIPS

Tip 1: Be cyber vigilant
Tip 2: Make simple decisions
Tip 3: Regularly review your crisis management plan
Tip 1: Be cyber vigilant
Tip 2: Make simple decisions
Tip 3: Regularly review your crisis management plan
Tip 4: Master your impact analysis
Tip 1: Be cyber vigilant
Tip 2: Make simple decisions
Tip 3: Regularly review your crisis management plan
Tip 4: Master your impact analysis
Tip 5: Communicate!
QUESTIONS?