STAMP-based Approach to Codifying the Lessons-learned from a Massive Leak of Personal Information from Japan Pension Service

Shigeru Kusakabe

University of Nagasaki, Japan

2017/Sep/15
Outline

• Introduction

• Incident

• Incident Reports

• Discussion

• Concluding remarks
Outline

• Introduction

• Incident

• Incident Reports

• Discussion

• Concluding remarks
Introduction

Objective:
• Demonstrate the effectiveness of STAMP as a more powerful alternative to conventional approaches in
  - explaining a security breach case, and
  - codifying lessons-learned

Method:
• Translate three different versions of incident report from different agents in a natural language into
  STAMP modeling notation.

(This Not CAST)
Incident overview

• In May 2015, the Japan Pension Service (JPS) was cracked.
• 124 malicious emails were sent since 8th May. Five staffs opened and 31 PCs were infected.
• It resulted in a massive leak of personal info. of 1.25 million enrollees, from 21th to 23th May.
• This prompted the revision of a new cyber-security strategy of the Japanese government.
Part of an extensive operation?

• Money was not the objective? The information stolen is not enough for financial attack.
  - 4-tuple: name, postal address, date of birth, and pension number. (52 thousands)
  - 3-tuple: name, date of birth, and pension number. (1.17 M)
  - 2-tuple: name and pension number. (31 thousands)

• Hackers seemed to shift their targets from the government to its peripherals
  - government-affiliated organizations, think tanks, private companies working with the government, and universities.
  - internal information hacked may be used as an inroad to other agencies and organizations.

• A far more serious incident at around the same time
  - The hack of the US Office of Personnel Management, resulted in the theft of data on 22.1 million employees, including millions with security clearance.
Outline

• Introduction

• Incident

• Incident Reports

• Discussion

• Concluding remarks
Government guideline existed

- The government guideline of security management assumed the following organizational interaction structure should work.

*NISC: National center of Incident readiness and Strategy for Cybersecurity

Intra organization level one also existed

JPS

Not covered explicitly

government-affiliated corporation
Main & Sub Agents (Components)

NISC: National center of Incident readiness & Strategy for Cybersecurity

MHLW: Ministry of Health, Labor & Welfare

JPS: Japan Pension Service

Contractor company of JPS (Outsourceree)
These systems manage personal information and are isolated from Internet.

- NISC monitors MHLW Net
- JPS LAN is connected to MHLW Network as it has strong relation to MHLW
<table>
<thead>
<tr>
<th>Date</th>
<th>Attack</th>
<th>JPS</th>
<th>MHLW</th>
<th>NISC</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/08</td>
<td>*Malicious mail1 to public address</td>
<td>*A staff clicked a link in malicious email. *Specified &amp; disconnected PC *URL block and warn all staffs() *Internal information might be stolen</td>
<td>*Notified JPS only (failed to report to MHLW supervisor)</td>
<td>*Detected suspicious comm. &amp; notified MHLW of it</td>
</tr>
<tr>
<td></td>
<td>*Malicious com. in 4 hours</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/15</td>
<td>*Thought “terminated” according to analysis of outsourcee</td>
<td></td>
<td></td>
<td>*Analyzed given malware-1, and notified MHLW of result</td>
</tr>
<tr>
<td>05/18</td>
<td>*Malicious mail2 /mail3 to private addresses</td>
<td>*3 staffs opened attached file of email and failed to detect infection *Reported to MHLW &amp; filed claim to Police</td>
<td>*No sense of crisis almost no actions</td>
<td></td>
</tr>
<tr>
<td>05/19</td>
<td>*Malicious mail4 to public address *C&amp;C server</td>
<td>*A staff opened attached file, PC infected, administrative information started stolen *Not aware of the staff’s behavior.</td>
<td>*Analyzed given malware-2&amp;3, and notified MHLW of result</td>
<td></td>
</tr>
<tr>
<td>05/20</td>
<td>*Leakage started</td>
<td>*26 PCs infected in total.</td>
<td>*Notified JPS only</td>
<td>*Analyzed given malware-4, and notified MHLW of result</td>
</tr>
<tr>
<td>05/22</td>
<td>*Specified &amp; disconnected PC, and closed the branch connection using MHLW net.</td>
<td></td>
<td>*Notified JPS only</td>
<td>*Detected suspicious comm. and notified MHLW of it</td>
</tr>
<tr>
<td>05/23</td>
<td>*Leakage stopped</td>
<td>*Specified &amp; disconnected PC according to warning of malicious communication from outsourcee. *Closed internet connection of the branch using MHLW network.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/28</td>
<td>*police told “we find stolen data”</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/29</td>
<td>*Stopped the entire internet connection using MHLW network</td>
<td></td>
<td>*Notified NISC of circumstances</td>
<td>*Raised priority and sent CYMAT to JPS</td>
</tr>
<tr>
<td>06/01</td>
<td></td>
<td></td>
<td></td>
<td>*Held high-level meeting and warned to all ministries</td>
</tr>
</tbody>
</table>
Outline

• Introduction

• Incident

• Incident Reports

• Discussion

• Concluding remarks
Different versions of report

NISC: National center of Incident readiness & Strategy for Cybersecurity

MHLW: Ministry of Health, Labor & Welfare

Independent team ordered by MHLW

JPS: Japan Pension Service

Contractor company of JPS (Outsourcer)
NISC version

• Committee:
  - Unknown inside NISC.

• Volume:
  - 26-page natural language document including one table and three figures.

• Feature:
  - No specific conclusions.
  - Mainly explaining technical facts and corresponding actions of NISC.
  - Also explaining usage of the government guideline, including suggestions for MHLW and JPS. (implicitly also for all government and affiliated organizations)
  - Including recurrence prevention measures for themselves.
JPS version

• Committee:
  - Five JPS members and one external lawyer.

• Volume:
  - 35-page natural language document plus 9-page appendix including two tables and one figure.

• Feature:
  - Most detailed one regarding JPS actions
    ✓ For example, actions in the following table.
    ✓ A little defensive, seeming like an excuse.
  - Recurrence prevention measures include JPS culture
    ✓ Incident management organizational system
    ✓ File server system
    ✓ Security policy
    ✓ Staff education
    ✓ Governance, culture
## Actions in JPS/targeted attack email

<table>
<thead>
<tr>
<th>Action</th>
<th>mail(1)</th>
<th>mail(2) 5/18</th>
<th>mail(3) 5/18_19</th>
<th>mail(4) 5/19</th>
<th>mail(5) 5/20</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor incoming email</td>
<td>△</td>
<td>O</td>
<td>△</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Specify range of mail recipient</td>
<td>X</td>
<td>O</td>
<td>△</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Disconnect PC if infected</td>
<td>△</td>
<td>X</td>
<td>X</td>
<td>O</td>
<td>X</td>
</tr>
<tr>
<td>Block the sender</td>
<td>X</td>
<td>O</td>
<td>△</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Notify overall members</td>
<td>△</td>
<td>△</td>
<td>△</td>
<td>△</td>
<td>X</td>
</tr>
<tr>
<td>Collect infected PC &amp; malware</td>
<td>O</td>
<td>O</td>
<td>△</td>
<td>X</td>
<td>O</td>
</tr>
<tr>
<td>Order virus analysis</td>
<td>O</td>
<td>△</td>
<td>△</td>
<td>NA</td>
<td>△</td>
</tr>
<tr>
<td>URL filtering</td>
<td>O</td>
<td>X</td>
<td>X</td>
<td>NA</td>
<td>X</td>
</tr>
<tr>
<td>Use vaccine</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>NA</td>
<td>O</td>
</tr>
<tr>
<td>Disconnect private line for email</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

〇 - properly taken, △ - slightly late, or partial, X - too late, no action
# Actions for suspicious communication

<table>
<thead>
<tr>
<th>Action</th>
<th>Suspicious communication (1) 5/18</th>
<th>Suspicious communication (2) 5/22</th>
<th>Suspicious communication (3) 5/23</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Monitor communication</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>2 Specify and disconnect infected PC</td>
<td>○</td>
<td>○</td>
<td>△</td>
</tr>
<tr>
<td>3 Analyze infection route</td>
<td>○</td>
<td>○</td>
<td>△</td>
</tr>
<tr>
<td>4 Analyze infected range using log</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>5 URL filtering</td>
<td>○</td>
<td>△</td>
<td>○</td>
</tr>
<tr>
<td>6 Enhance communication monitoring</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>7 Collect PC with malware</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>8 Order virus analysis</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>9 Use vaccine</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>10 Disconnect private line for email</td>
<td>X</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>11 Disconnect all lines for internet</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

- ○ - properly taken, △ - slightly late, or partial, X - too late, no action
Violation of Operation Rule

This system was cracked.

These systems manage personal information and are isolated from Internet.

Manually copied!
Independent team version (MHLW)

• Committee:
  - 19 members (lawyers, security experts, auditors, …)

• Volume:
  - 37-page natural language document plus 3-page glossary.

• Feature:
  - Most comprehensive one
  - Interviewed 78 people and analyzed documents: MHLW, JPS, and its outsourcee and security soft company.
  - Tried to find “root cause”
    ✓Lack of security risk awareness for their situation, security trend
    ✓Inappropriate management system.
  - Recurrence prevention measures also include JPS culture
    ✓Management system in JPS
    ✓Management system in MHLW
    ✓Technical measures
    ✓Culture in JPS

Sep/15/2017
ESW2017 © Shigeru Kusakabe
Outline

• Introduction
• Incident
• Incident Reports
• Discussion
• Concluding remarks
Discussion

• JPS and MHLW were so immature before and during the incident.
• We will find many missing control actions, actuators, sensors, feedbacks, process models in a visual manner if we use STAMP.
Why?

Using STAMP makes me consider why this could happen. Most of the issues are related to inter/intra-organizational management system. Let’s consider Japan specific issues

• We Japanese tend to communicate in high-context, with fewer words but a sort of telepathy.
  - Tend to avoid explicitly clarify responsibility and requirements.
  - Request for clarification may be regarded as arrogant/offensive.
  - Unrealistically optimistic expectation/assumption may survive.

• Seniority system still exists.
  - Our boss may have no knowledge nor mind set for emerging issues like security. This makes things like above much worse.

• “Amakudari” & “Sontaku” in organizations like JPS
  - Amakudari: Descent from heaven, revolving door, …
  - Sontaku: Required to behave by reading between lines.
Is it a better language in describing & analyzing security management in a constructive way (especially for Japanese)?

Linguistic (model) relativity
“The principle of linguistic relativity holds that the structure of a language affects its speakers' world view or cognition.”
(Wikipedia)
Proof of Concept needed (Plan)

Sample: Japan Information Security Audit Assoc.

• Audit method
  - Hearing
  - Review
  - Observation
  - Test

• Audit procedure guideline

<table>
<thead>
<tr>
<th>Management details</th>
<th>Target</th>
<th>Method</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>Responsibility of executives and organizational efforts for security management are written in the security policy documents</td>
<td>Security policy documents</td>
<td>Review</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Outline

• Introduction

• Incident

• Incident Reports

• Discussion

• Concluding remarks
Summary

Trial Results:
• The insufficient inter/intra-organization controls can be represented in a structured & hierarchical way.
• It helps to explain the unsecure behaviors although additional context information will facilitate understanding of the reasons behind the behaviors.

Conclusions:
• STAMP seems more effective than conventional natural language based approach in representing & assessing the organizational control structure.
• We will continue this work by collaborating with practitioners such as auditors.