Information Security and Data Privacy

Phishing Incident Response

Play Book

Revision 1.0

7/24/2018

Effective date *(update for each revision)*	**Document Owner**	**Document ID**
7/24/2018	Igor Spektor	900

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Phishing Incident Response Play Book should be retained in hard copy format in case Global Eagle Entertainment online systems are unavailable during an Incident

1 Table of Contents

2 Copyright, Trademarks, Notice of Proprietary Rights

2.1 COPYRIGHT

Information in this document may change without notice and does not represent a commitment on the part of Global Eagle™.

Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice. The claim of copyright does not imply waiver of Global Eagle's other rights. See notice of Proprietary Rights.

2.2 TRADEMARKS

The Global Eagle™ logos are registered trademarks of Global Eagle™.

All other company and product names used herein may be the trademarks or registered trademarks of their respective companies.

2.3 NOTICE OF PROPRIETARY RIGHTS

This documentation is a confidential trade secret and the property of Global Eagle™ and contains Global Eagle's Confidential, Proprietary, or Privileged Information. Use, examination, reproduction, copy, de-compilation, transfer, and disclosure to others are strictly prohibited except by express written agreement with Global Eagle™.

3 Revision History

Date	Version	Prepared By	Document Changes
7/24/2018	Revision 1.0	Stephen Mitchell	Initial Draft

Table 1: Revision History

4 Approvals

Name	Title	Reviewed By	Approved By	Date
Igor Spektor	Head of Information Security and Compliance	Igor Spektor		7/24/2018
Dmitry Chausovsky	Head of Compliance and Privacy	Dmitry Chausovsky		7/24/2018

Table 2: Approvals

5 Points of Contact

Name	Title	Email	Contact Number
Igor Spektor	VP, Head of Information Security and Compliance	Igor.Spektor@globaleage.com	+1-954-401-9155
Dmitry Chausovsky	VP, Head of Compliance and Privacy	Dmitry.Chausovsky@globaleagle.com	+1-310-740-8611

Table 3: Points of Contact

6 Introduction

6.1 Audience

This document is intended for use by Global Eagle Entertainment Inc. and its subsidiaries (Global Eagle)'s management, employees, external auditors, risk advisors, outside labor and service providers, globally.

6.2 Assumptions

This document is reviewed (at least annually) and updated as appropriate.

6.3 Owner and Contact

No material part of this document is to be altered without the agreement of Global Eagle Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Head of Compliance and Privacy. All updates to this document must be implemented using proper change control.

6.4 Distribution

This is an electronically controlled and issued document. The latest electronic version of the document is available at the Global Eagle™ Information Technology page here. Users should always confirm they are using the latest electronic version of the document.

.

7 Phishing Play Book Definition:

7.1 Purpose of Phishing Incident Report Play Book:

This document defines and describes the procedures when phishing incidents happen. This file allows responders to follow a structured methodology for validating and responding to each unique security alerts related to Phishing Emails.

7.2 Scope:

Any phishing related events that identified during daily Security operations or is escalated to IRT (Incident Response Team). IRT is responsible for maintenance activities including reviews and revisions.

7.3 Phishing Definition:

Email threats are when an attacker attempts to collect sensitive information such as usernames, passwords, credit card details, Social Security Numbers, Protect Health Information and other personal or protected data, often for malicious reasons, by masquerading as a trustworthy entity in electronic communication. The term is sometimes confused with emails that contain malware intended to infect the recipient's system; however, the appropriate term for those types of emails is "malspam" or "Malicious SPAM Emails." Those types of events should follow the Malicious Code Playbook.

8 Identifying phishing Email:

Following statements may be used as a guide to assist with determining the nature of a Phishing incident:

- Any emails that result in loss or damage to the Company or client information assets.
- Any Infected files or links inside the email that result in loss or damage to the Company or client information assets.
- Any emails that result in Compromised accounts of clients.
- Any suspicious Email address which can cause one of the mentioned issues.

9 Process Summary:

The workflow below shows stages of the Email Threats Incident response:

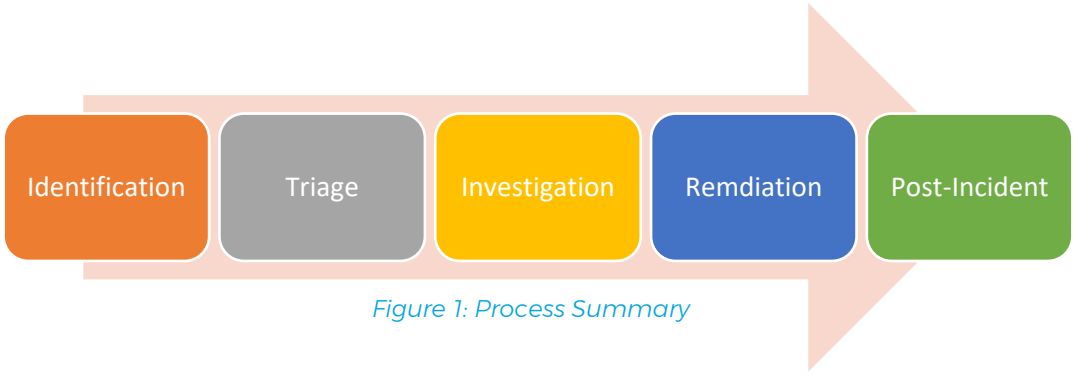


Figure 1: Process Summary

Post-Incident Process	Description
Identification	This stage includes the identification and initial scoping of a security alert.
Triage	This stage includes verifying if the security alert is an incident, the severity of the event, and additional analysis.
Investigation	This stage involves investigating the security incident in detail, ensuring all information is documented. Additionally, the investigator will have fully scoped the incident by the end of this stage.
Remediation	This stage includes containment and remediation steps for mitigating and eradicating the threat.
Post-Incident	This stage includes a final review of the investigation record by the L2 – Incident Specialist, ensuring nothing was overlooked. Once completed, the record is closed.

Table 4: Post Incident Response

9.1 Identification

(L1 – IRT) Identification	Description
Alert Sources	— SIEM —Outlook ATP —End Point Protection(McAfee) —IPS —Firewalls —Clients —UgovernIT —Phishing Report Emails
Procedures	1. **Initial Alert:** Alerts – L1 will be alerted to potential suspicious emails from sources. 2. **Create an Investigation Record.** An investigation record is opened for each discrete alert within the UgovernIT, and all pertinent investigative data is recorded there. Duplicate events or events that are components of the same investigation can be aggregated in a previously opened case, provided the investigation record is still in the opened state. 3. **Validate that the original message headers are present.** The L1 initially inspects the email message's original headers. To do so, the L1 must receive the original email sent to them as an attachment to a secondary email. If an email is received by using the email "forward" feature, the L1 must respond to the initial sender (i.e., the internal recipient of suspicious email) and request that they attach the original message to a new email as an attachment and send it to the <phishing.report@globaleagle.com> email. 4. **Message Data Gathering.** During the Data Gathering process, the L1 gathers relevant data regarding the alert based on the type of alert and the sources of information available to them. In the case of phishing, the following details should be collected: —Sender Email Address. —Recipient Email Address(es). —Subject Line. —Sending server IP Address. —X-Originating-IP (or similar, if available)

(L1 – IRT) Identification	Description
Procedures	During the Data Gathering process, the L1 gathers relevant data regarding the alert based on the type of alert and the sources of information available to them. In the case of phishing, the following details should be collected: —Sender Email Address. —Recipient Email Address(es). —Subject Line. —Sending server IP Address. —X-Originating-IP (or similar, if available). 5. Record Message Delivery Ratio and Impacted Users. Perform a query on Outlook for related messages. Search based on unique identifiers that will identify all email messages in the phishing campaign. Multiple searches may be necessary, as a simple search by Subject or Sender may not identify all related messages from the campaign. Attackers will vary in fields, such as using different subject lines throughout the duration of a campaign to evade detection. In the case of phishing, the following details should be collected: —A number of emails in the campaign that successfully bypassed Outlook ATP. —A number of emails in the campaign blocked by ATP. —Record User IDs of users that received the phishing email. 6. Email Attachment Collection. If the original email message contains a file attachment, collect the file safely and store it within a password protected zip-file, using the password 'infected.' Attach this file to the investigation record. 7. Domain & URL Profiling. Profile the domain and URL that is contained within the message (if applicable): —Record the full URL to the phishing webpage. —Record VirusTotal.com results by searching the URL. —Submit the attached file to Virus total and record the results

(L1 – IRT) Identification	Description
Procedures	—Submit URL to URLVoid.com and record Safety Reputation score and Report URL. —Submit IP address to IPVoid.com and record Detection Ratio and Report URL. —Use http://www.toolsvoid.com/whois-lookup to search the WHOIS registration information, save it in a TXT file and attach it to the investigation record. —Search the URL on PhishTank.com to validate if it has already been reported as a Phish. —Additionally, search the URL or any related IP addresses using https://otx.alienvault.com or https://exchange.xforce.ibmcloud.com and report the URL and findings in the investigation record. 8. **Escalate.** The L1 escalates the investigation to the L2 – IRT

Table 5: (L1 – IRT) Identification

9.1 Triage:

The Triage stage deals with verifying if the security alert is an incident, the severity of the event, and additional analysis.

(L2 – Incident Analyst) Triage	
Relevant Tools	—UgovernIT —Outlook ATP —Dynamic malware analysis sandbox
Procedures	1. **Known False Positive.** If this alert is a known false positive that is in progress of being tuned out, close the investigation at this point. 2. **Phishing Email vs. Malicious Email.** Based on inspection of the message, does the message constitute a phishing email, or an email containing malware or links to malicious code? If applicable, submit the email attachment (previously attached to the investigation record) to the dynamic malware analysis sandbox and attach the resulting report to the investigation record. 3. **Spear-Phishing Email Verification.** Does the email appear to be sophisticated and highly targeted at the organization and any specific individuals? Does the phishing campaign follow any of these attributes? (not limited to): —A small number of users received the email. —Not a generic mass-mail type message (e.g., mentions our organization). —Impersonation of anyone within our organization. —Embedded links or attachments are purporting to be documents related to our organization. If the email is deemed to be highly targeted, refer to the Targeted Attack Playbook. 4. **Declare Incident, Determine the Incident Priority, and Open the Incident Ticket.** Use the Incident Priority table to calculate a priority rating for this case based on the available information collected during the first two phases of the investigation. Open an Incident Ticket in UgovernIT. 5. **Escalate.** If the Incident Priority rating is 4 or 5, escalate the incident to the L2 – IRT for further investigation.

Table 6: (L2 – Incident Analyst) Triage

Incident Calculator Matrix:

	High(3)	Medium(2)	Low(1)
Significant/ Large(3)	Highest priority(6)	High priority(5)	Low priority(4)
Moderate/ Limited(2)	High priority(5)	Medium priority(4)	Lowest priority(3)
Minor/ Localized(1)	Medium priority(4)	Low priority(3)	Lowest priority(2)

Table 7: Incident Calculator Matrix

Urgency	
High	If the email causes significant security issue: getting access to classified documents, getting admin access or changing configuration, compromised accounts (more than1), sending emails from employees inboxes
Medium	If the email causes medium security issues: compromised account, limited access to clients, installing malware
Low	Phishing emails which make suspicious activities as traffic, suspicious file, unusual performance

Table 8: Urgency

Impact	
Significant	If the email causes risks to more than ten employees
Moderate	If the email causes risks for two-ten employees
Minor	If the email causes risks for one person

Table 9: Impact

9.2 Investigation

The Investigation stage deals with investigating the security incident in detail, ensuring all information is documented. Additionally, the investigator will have fully scoped the incident by the end of this stage. Identification.

(L2 – Incident Analyst) Investigation	
Relevant Tools	—McAfee) —Firewalls/IPS —ATP —Cisco Umbrella/Websense —Wireshark
	1. **Analyze Email Header.** Examine the email header for the following phishing attributes: —Return-Path field contains an email address that is not related to the name shown in the **From** field in the original email. —The X-Authenticated-User field contains an email address which appears suspicious (e.g., johnsmith@unknowndomain.ru). —The Mail Server IP address in the header is known to be malicious. ▪ Search the IP address on http://mxtoolbox.com/blacklists.aspx —The email domain is known to be malicious. o Search the domain on https://www.ultratools.com/tools/spamDBLookup. Email header details, including external tool search results, must be recorded in the investigation record. 2. **Determine the Phishing Page Submission URL.** Analyze the phishing page URL and determine where the page posts the related data. **Option 1:** —Load the URL in **ToolsVoid** URL Content Dump: http://www.toolsvoid.com/url-dump. —Copy and paste the contents from the “Downloaded RAW Data” section into http://jsbeautifer.org/ and click “Beautify JavaScript or HTML.” —Copy the beautified data into a text editor (e.g., Notepad++) for analysis.

(L2 – Incident Analyst) Investigation	
	—Search for the FORM object. Typically, a search for <form will identify this quickly. Ensure you are looking at the form that has the **method="post"** and is the main submission form, not a search bar or some other form on the page. — Read the action parameter and determine the URL where the form is being posted. — Record this URL in the investigation. **Option 2:** — Open the URL in your browser and prepend the phrase "view." **Option 3:** — Start **Wireshark** and commence a Packet capture (disable Promiscuous Mode). — Access the Phishing URL in a web browser with JavaScript enabled. — Fill in the Phishing page form with false data and submit the form. — Close the page and stop the packet capture. — Apply a filter in **Wireshark** for http.request.URI contains "phishing domain." ▪ The quotation marks are important, and the content within them should be the actual domain from the investigation and not the words phishing domain. — This identifies the initial request made by the user when loading the phishing form page. — Click on the line item, note the packet number, and clear the filter. — Review the following lines of traffic to understand where the request was submitted. — Apply a filter in **Wireshark** for **http.request.method == POST**. — This identifies the POST request made by the user when submitting the form. — Alternatively: — Click **File**. — Click **Export Objects** (near the bottom). — Select **HTTP**. — Once the packets have been processed, a dialog box will appear labeled "Wireshark: HTTP object list."

	▪ Review the list for a quick summary view of the HTTP transactions that occurred during the packet capture. ▪ Identify the traffic that immediately follows the access to the phishing domain. 3. **Review Proxy Logs for Evidence of Access to Phishing Page URL.** Run a Websense/Cisco Umbrella report summarized by the user with the verdict "Allowed" on the domain hosting the phishing page. Record the list of user IDs in the investigation record. 4. **Affected User Profiling.** Profile the users that have clicked through to the submission page and record this information in the investigation record. — Record User ID. — Look up and record the user's name, title, department, physical location. 5. **Escalation Verification – Recalculate Priority Rating.** Using the information that has been gathered at this point, recalculate the incident priority rating using the Excel-based Incident Priority Calculator. If the priority has been raised to 6,7 or 8 escalate to the L2.

Table 10: (L2 – Incident Analyst) Investigation

Remediation Stage:

The Remediation stage deals with containment and remediating steps for mitigating and eradicating the incident.

(L2 – Incident Analyst) Remediation	
Relevant Tools	—UgovernIT —McAfee —Cisco Umbrella/Websense —Firewall/IPS —Outlook ATP —PhishTank
Procedures	1. **Implement an ATP Block.** Create a blocking rule on future messages of this type. If ATP is unable to provide an explicit block on these exact messages from being received in the future, implement a custom rule to prevent further messages matching the sample email. Responsible: ATP Admin. 2. **Update Cisco Umbrella/Websense.** Submit the URL of the phishing page to Cisco Umbrella/Websense for categorization. Responsible: Websense/Cisco Umbrella Admins. 3. **Submit URL to PhishTank.** Submit the URL of the phishing page to **PhishTank** for categorization. Responsible: L2 IRT. 4. **Change Affected User's Credentials.** Affected users should change their passwords for all systems that may have been compromised by the information submitted to the phishing submission page. Responsible: Help Desk Supports. 5. **Monitor System and User Account for Possible Misuse.** Monitor the system and user account of the victim of the phishing attack for any possible misuse related to the possible harvesting of credentials associated to the phishing attack. **Responsible: ATP Admins, L2 IRT, Admins of Firewalls, Help Desk Supports.** 6. **Update the Investigation Record.** The investigation record will be updated with all actions performed.

	Responsible: L2 IRT

Table 11: (L2 – Incident Analyst) Remediation

Response time:

After issuing ticket or emails for remediation, all requested actions must be done before the deadline:

ID	Priority	Deadline
1	Highest Priority	2 hours
2	High Priority	2-4 hours
3	Medium Priority	24 hours
4	Low Priority	48 hours

Table 12: Response time

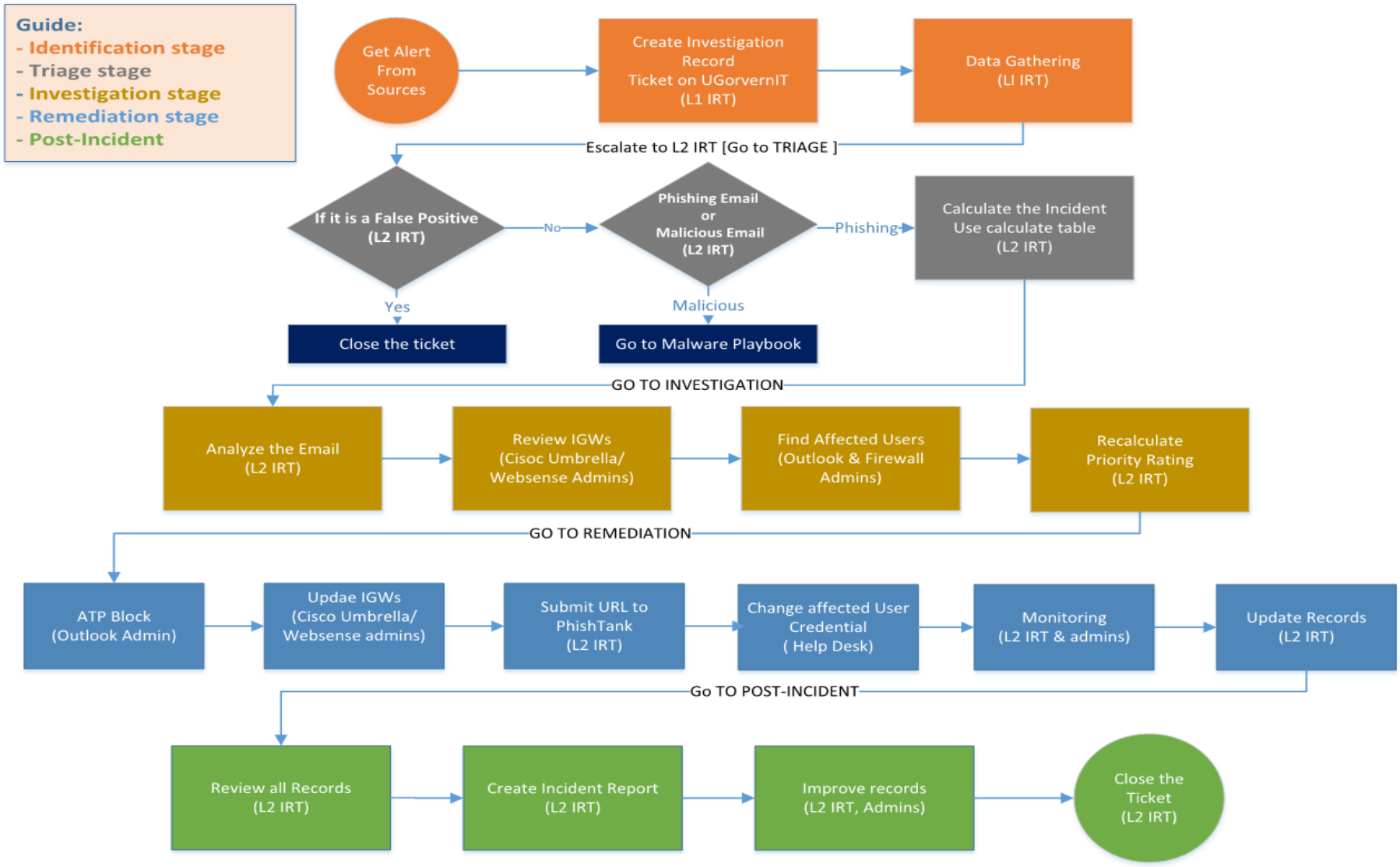
(L2– IRT) Post-Incident	
Alert Sources	—UgovernIT
Procedures	1. **Review Investigation Record.** Review the investigation record and verify that all pertinent information, including details about the investigation as well as steps taken by the investigator, are recorded accurately. 2. **Create an Incident Review Report.** Provide Incident report for incidents with 8 or 7 scores. 3. **Improve/Update.** Determine if there were an area(s) for improvement or if updates are needed: i. Update documentation (e.g., use cases, playbooks). ii. Create new Alerts as needed. iii. Review Technical & Policy Controls - Review additional. 4. **Close the Investigation Record.** Resolve the ticket on UgovernIT.

Table 13: (L2– IRT) Post-Incident

:

10 Appendix

10.1 Phishing Incident Response Play Work Flow


Guide:
- Identification stage
- Triage stage
- Investigation stage
- Remediation stage
- Post-Incident
Get Alert From Sources
Create Investigation Record Ticket on UGorvernIT (L1 IRT)
Data Gathering (LI IRT)
Escalate to L2 IRT [Go to TRIAGE]
If it is a False Positive (L2 IRT)
No
Phishing Email or Malicious Email (L2 IRT)
Phishing
Calculate the Incident Use calculate table (L2 IRT)
Yes
Close the ticket
Malicious
Go to Malware Playbook
GO TO INVESTIGATION
Analyze the Email (L2 IRT)
Review IGWs (Cisoc Umbrella/ Websense Admins)
Find Affected Users (Outlook & Firewall Admins)
Recalculate Priority Rating (L2 IRT)
GO TO REMEDIATION
ATP Block (Outlook Admin)
Updae IGWs (Cisco Umbrella/ Websense admins)
Submit URL to PhishTank (L2 IRT)
Change affected User Credential (Help Desk)
Monitoring (L2 IRT & admins)
Update Records (L2 IRT)
Go TO POST-INCIDENT
Review all Records (L2 IRT)
Create Incident Report (L2 IRT)
Improve records (L2 IRT, Admins)
Close the Ticket (L2 IRT)

11 Table of Figures

12 Table of Tables