Computer Incident Response Team
Role in Combating Cybercrime

Mohamad Sazly B Musa
IMPACT
22nd September 2011
Agenda

1. Overview of Cyber Crime
2. Statistics
3. Fighting Cyber Crime
4. The Role of CIRT
5. Why Establish CIRT?
6. Benefits of CIRT
7. CIRT Initiatives
8. Legal Basis for Collaboration
9. Conclusion
Cyber Crime: Definition

“Criminal acts using computers and networks as tools or targets”

The use of a computer to achieve illegal ends
Types of Cyber Crime

- **Computer Related**
  - Hacking
  - Viruses & worms
  - DDoS
  - Web defacement
  - Phishing
  - Espionage
  - Identity theft
  - Credit card frauds

- **Copyright Related**
  - Software piracy
  - P2P

- **Content Related**
  - Pornography
  - Online gambling
  - Spam

- **Combination Offenses**
  - Cyberterrorism
  - Attacks on Government Infrastructure
  - Cyber laundering
Challenges

• Before
  – Nearly all crimes were local
  – Evidence never far from the crime scene

• Now
  – Internet crimes span multiple jurisdiction
  – Specialised procedures & forensics
  – Evidence across borders
  – How to get Legal Assist across borders
Scope of Cyberspace

Cyberspace starts with the internet...

Network of networks
= Internet
Modern Weapons Economics

What does a stealth bomber cost?  
$1.5 to $2 billion

What does a stealth fighter cost?  
$80 to $120 million

What does a cruise missile cost?  
$1 to $2 million

What does a cyber weapon cost?  
$300 to $50,000
Cyber Crime Statistics 2010

Internet Crime Complaint Centre

Figure 2: Yearly Comparison of Complaints Received Via the IC3 Website

Hacktivist

- Hacking refers to unlawful access to a computer system
- One of oldest computer related crimes

Anonymous Group

Lulz Security
Anonymous Activities

• Operations Payback, Avenge Assange, and Bradical - Dec 2010
  – To support WikiLeaks and launched DDoS attacks against Amazon, PayPal, MasterCard, Visa and the Swiss bank Post Finance

• Operation Sony 2011
  – To attack Sony websites in response to Sony's lawsuit against George Hotz
Anonymous Activities

• Operation Malaysia - June 2011
  – Launched attacks on ninety-one websites of the Malaysian government in response to the blocking of file sharing websites

• Operation Anti-Security - July 2011
  – The group has teamed up with LulzSec to hack the websites and release information from a large number of government and corporate sources.
Strategy to Fight Cyber Crime

• Technology
  – The quality of software needs to improve

• Education
  – To raise the risk awareness of the everyday visitor in cyberspace

• Legal Frameworks
  – Legislation that keeps up with the current challenges of cybercrime must exist and continually evolve.

• International Cooperation
  – To improve international cooperation and mutual assistance on cybercrime among governments, industry and non-governmental organisations (NGOs)
The Role of CIRT

- Cybercrime is a global problem, so it goes without saying that it needs a global response.
- Need to build up national cyber defense
  - CERTs, CSIRTs, national security agencies, etc.
  - Improve incident response capability – how fast can we respond to attack
- CIRT can provide a single point of contact for dealing with cyber security incidents
Why Establish CIRT?

• Motivators driving the establishment of CIRT:
  – Increase in the number of reported computer security incidents
  – Growth in the number of reported vulnerabilities
  – The realisation that system and network administrators alone cannot protect organisational systems and assets
  – The realisation that a prepared plan and strategy is required
  – To encourage citizens and companies to report crimes more often
CIRT Functions

• Provides a single point of contact for reporting security incidents
• Assists the organisational constituency and general computing community in preventing and handling computer security incidents
• Shares information and lessons learned with other response team
• Collaborate with law enforcement agencies and local authority bodies
CIRT Functions

It is critical that mechanisms are in place to:

• Provide early warnings
• Effectively detect & identify the activity
• Develop mitigation & response strategies
• Establish trusted communications channels
• Effect a coordinated response
• Share data & information about the activity
• Track & monitor this information to determine trends & long term remediation strategies
Benefits of CIRT

- Serve as a trusted point of contact
- Develop an infrastructure for coordinating response
- Develop a capability to support incident reporting
- Conduct incident, vulnerability & artifact analysis
- Participate in cyber watch functions
- Help organisations to develop their own incident management capabilities
- Provide language translation services
- Make security best practices & guidance available
- Provide awareness, education & trainings
CIRT Initiatives

• India, US join hands to fight cyber crime, sign MoU
  – To enable exchange of critical cyber security information and expertise between the two governments through the CERT-In and US Computer Emergency Readiness Team (US-CERT)

• The Government of Luxembourg presented the new Cybersecurity board and the "Computer Emergency Response Team", in the effort to anticipate and fight virtual attacks.  (http://www.investinluxembourg.lu/ict/new-strategy-prevent-and-fight-cybercrime)
CIRT Initiatives

- EU prepares to set up Computer Emergency Response Team
  (http://www.infosecurity-magazine.com/view/18608/eu-prepares-to-set-up-computer-emergency-response-team)
  - The European Union has set up a team to establish a Computer Emergency Response Team (CERT) to counter the threat of cyber attacks against EU institutions, bodies and agencies.

- East Africa to fight cybercrime with CERT
  (http://news.idg.no/cw/art.cfm?id=CBB60BB2-1A64-6A71-CEB17DB32C209CD3)
  - A plan for the five East African states of Uganda, Kenya, Tanzania, Rwanda and Burundi to set up Computer Emergency Response Teams (CERTs) to fight cybercrime is under way, as countries involved seek to involve the ITU's help.
Workshops & CIRT Deployment

Objectives:
- To assist partner countries’ assessment of its readiness to implement a National CIRT.
- IMPACT reports on key issues and analysis, recommending a phased implementation plan for National CIRT.
- In later stages the national CIRT will also be provided with enabling tools.
- Conducted workshops for 24 countries globally

<table>
<thead>
<tr>
<th>No.</th>
<th>Partner Countries</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Afghanistan</td>
<td>Completed in October 2009</td>
</tr>
<tr>
<td>2</td>
<td>Uganda, Tanzania, Kenya &amp; Zambia</td>
<td>Completed in April 2010</td>
</tr>
<tr>
<td>3</td>
<td>Nigeria, Burkina Faso, Ghana, Mali, Senegal &amp; Ivory Coast</td>
<td>Completed in May 2010</td>
</tr>
<tr>
<td>4</td>
<td>Maldives, Bhutan, Nepal &amp; Bangladesh</td>
<td>Completed in June 2010</td>
</tr>
<tr>
<td>5</td>
<td>Serbia, Montenegro, Bosnia &amp; Albania</td>
<td>Completed in November 2010</td>
</tr>
<tr>
<td>6</td>
<td>Cameroon, Chad, Gabon, Congo &amp; Sudan</td>
<td>Completed in December 2010</td>
</tr>
<tr>
<td>7</td>
<td>Cambodia, Vietnam, Myanmar</td>
<td>Under Assessment Currently</td>
</tr>
<tr>
<td>8</td>
<td>Armenia</td>
<td>Planned for October 2011</td>
</tr>
<tr>
<td>9</td>
<td>Laos</td>
<td>Assessment in September 2011</td>
</tr>
<tr>
<td>10</td>
<td>Montenegro, Kenya, Zambia, Nigeria, Uganda</td>
<td>Deployment in 2011-12</td>
</tr>
</tbody>
</table>
Legal Basis for Collaboration

• Need to improve on the standard collaboration documents for the different CIRTs due to a wide diversity in the legislation
  – Standard Non Disclosure Agreement (NDA)
  – Standard Acceptable Use Policy (AUP)
  – Terms of Reference (ToR)
  – Standard Service Level Agreement (SLA)
  – Collaboration Agreements
    ▪ Memorandum of Understanding (MOU)
    ▪ Contract
Conclusion

• Cyber security is a global problem that has to be addressed globally by all governments jointly
• No government can fight cybercrime or secure its cyberspace in isolation
• International cooperation is essential to securing cyberspace
• It is not a technology problem that can be ‘solved’; it is a risk to be managed by a combination of defensive technology
Thank you
mohamad.sazly@impact-alliance.org
www.facebook.com/impactalliance