Cybersecurity for the Americas
ITU Regional Event
“Connecting the World Responsibly”

Michael Lewis, Consultant to the ITU
General Trends

- Users on Internet
- Computers
- Devices
- Core Applications
  - eGov, CII
- Vulnerabilities
- Exploits
- Financial Incentives
- Criminal Activity
- & consider political motivations!
The Dynamics of CyberCrime

- Barriers to entry are minimal
  - resources are essentially free (!)
  - technical requirements are modest

- Low risk, high reward!
  - Opportunities grow with continued E-volution of services
  - Returns are tantalizingly large
  - Physical distance of criminal from the “scene” of the crime renders apprehension unlikely

- Prosecution is rare
  - Investigation is costly in time & resources
  - Challenging to trace and attribute
  - Coordination of investigations across borders is difficult

- Innovation seems to be more prevalent on the “dark” side – consider botnets!

  Cybercrime is a growth industry!
Considerations for the Workshop

- We are all doing something (because we have to!) but how well is it working?
- Is there a national strategy for cyber security, with policies, and operational capabilities? If so, is it coherent and compliant (?)?
- So many actors – How do we establish authority, roles, responsibilities, and coordination?
- So much data, and so many organizations - How and where to link and assimilate?
- When something goes wrong, who do you call?
Coordinating a National Approach to Cybersecurity

- Develop a national cybersecurity strategy and policies
  - It starts with a self-assessment of the current state of affairs
- For each actor, identify constituents and services
  - What do you do, and for whom? Are there gaps? Redundancies?
- Build trusted relations & secure mechanisms for collaboration with counterparts (national, regional, international)
  - In advance, not in times of crisis
- Establish relevant operational capabilities – such as Incident Management & Coordination
- Conduct regular, targeted events to build skills, test systems and escalation procedures, & share experience
- The work should be subject to ongoing self-assessment and course correction.
Computer Security Incident Response Team (CSIRT)

As many have noted, a “CSIRT” is one component of a national cyber security strategy

- aka, a Computer Emergency Response Team”
- aka, a Computer Incident Response Team
- aka, a Computer Incident Readiness Team
- Or, any number of variations!

Can exist within an organization, or at a national, regional, or global level

- Actually, at all levels, mutually reinforcing

Should be proactive more than reactive

- Note the reactive implications of most of the acronyms!
Why Build a CERT / CSIRT / CIRT?

- Cyber Security is important enough to receive dedicated personnel and resources
  - Rather than “oh, and you guys should do security, too”
- It can exemplify and propagate high-level policies and best practices
- It can formalize incident response and capture “lessons-learned” to improve policies and procedures
- It establishes responsibility, accountability, “accredited” points-of-contact, and reliable communication channels

Sort of a “Ghostbusters” for cyber incidents
### Range of Services

**as per the SEI of CMU**

<table>
<thead>
<tr>
<th>Reactive Services</th>
<th>Proactive Services</th>
<th>Security Quality Management Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Alerts and Warnings</td>
<td>+ Announcements</td>
<td>✓ Risk Analysis</td>
</tr>
<tr>
<td>+ Incident Handling</td>
<td>+ Technology Watch</td>
<td>✓ Business Continuity &amp; Disaster Recovery Planning</td>
</tr>
<tr>
<td>– Incident analysis</td>
<td>+ Security Audit or Assessments</td>
<td>✓ Security Consulting</td>
</tr>
<tr>
<td>– Incident response on site</td>
<td>+ Configuration &amp; Maintenance of Security Tools, Applications, &amp; Infrastructures</td>
<td></td>
</tr>
<tr>
<td>– Incident response support</td>
<td>+ Development of Security Tools</td>
<td>✓ Awareness Building</td>
</tr>
<tr>
<td>– Incident response coordination</td>
<td>+ Intrusion Detection Services</td>
<td>✓ Education/Training</td>
</tr>
<tr>
<td>+ Vulnerability Handling</td>
<td>+ Security-Related Information Dissemination</td>
<td>✓ Product Evaluation or Certification</td>
</tr>
<tr>
<td>– Vulnerability analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Vulnerability response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Vulnerability response coordination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+ Artifact Handling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Artifact analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Artifact response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>– Artifact response coordination</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Any given CSIRT is likely to implement only a subset of such services.
An Organizational CSIRT

Who do they call?

- end-user
- "first responder"
- Help Desk
  IT Department
  Network Ops

- Push Alerts, Updates, Patches
- Propagate and Enforce Policies
- Receive Reports
- Respond to Incidents!
- Observe Escalation Procedures
- Report as needed to national center

“Front-Line” Response
to formalize “internal” incident response
Note the “Forum of Incident Response and Security Teams”
A necessary but not sufficient component of a national cyber security strategy

Note the “CSIRTs with National Responsibility” working group
National CSIRT Activities
representative examples from recent work

- Launched an Outreach, Awareness, and Training group
  - Conducted dozens of specialized trainings and workshops
  - Worked with schools and universities to provide security material, lectures, and even shape course curricula
  - Established a cyber-security forum series
  - Hosted quarterly regional and international security events, such as an ITU regional workshop, a FIRST Technical Colloquium, and the inaugural Regional-CERT meetings
National CSIRT Activities
representative examples from recent work (2)

- Launched the national incident reporting and response center
  - Inaugurated national incident reporting and response
  - Encouraged the creation and ongoing support of organizational CSIRTs, with mutual p-o-c’s, key exchange, workshops
  - Built a state-of-the-art cyber-forensics lab
  - Provided training in policy and practice for national law enforcement
  - Conducted “incident response and engagement with law enforcement” program for constituents
  - Provided 24/7 technical back-stopping for high-profile national events
National CSIRT Activities
representative examples from recent work (3)

- Established a Critical Infrastructure Protection group
  - and “sector working groups”
  - and helped draft the national CIIP policy
  - to identify and propagate high-level practices, procedures, and compliance methods
A community with complementary and reinforcing roles and responsibilities, from end-user up to the national level.
Align & Partner

many good initiatives exist
Further Discussion Points

- Scaling of points-of-contact relations
- Confidence and discretion of national CERTs
- Incident Response vs. Cyber Forensics
- Incident Response & issues of authority, responsibility, liability, coordination
  - Ex. - “Takedown”
  - Ex. - Denial of Service
  - Ex. - Financial Fraud & balancing interests of law enforcement vs. that of various victims