Recall the Trends

- Users on Internet
- Computers
- Devices
- Core Applications
  - eGov, CII
- Vulnerabilities
- Exploits
- Financial Incentives
- Criminal Activity
- & consider political motivations!
We have established in recent sessions that...

- IT systems have become fundamental to the effective functioning of core societal services (eGov, eHealth, eEducation, eCommerce, Energy, Communications, etc.)
- and are too important to fail, thus should be considered elements of our national critical infrastructure
- yet disruptions happen, often, for myriad reasons, some malicious
- so we must establish an effective capacity to detect and respond to incidents (such as the CSIRT model) at the organizational and national levels, and coordinate this effort
- and learn from the experience to diminish the number and significance of future incidents
And further agreed that . . .

- Cyber Security is important enough to receive dedicated personnel and resources
  - Rather than “oh, and you guys should do security, too”
- A CSIRT 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
Any given CSIRT is likely to implement only a subset of such services
An Organizational CSIRT

Who do they call?

end-user

“front-line” response

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”
The Incident Response component of a CSIRT could include:

- **Watch** – to monitor threats & vulnerabilities, and assess relevance and risk
- **Warning** – to disseminate validated threats to at-risk constituents
- **Investigation** – to analyze how an incident occurred, for technical and possibly legal reasons
- **Response** – to detect and mitigate potentially disruptive incidents
Watch

Monitor Inputs

- hardware system announcements
- vulnerability reports
- software updates
- patch releases
- security tool updates
- targeted threats (e-mail, blogs)
- Network traffic anomalies (netflow and honeynet data)
- Early Warning and Alerts

CSIRT
Assess and filter “Watch” inputs and disseminate relevant reports

“Watch” feeds

CSIRT

Constituents

Alerts and technical advice
Investigation

- Gather and review the “artifacts” of an incident
- Review timeline and sequence of events
- Analyze factors that contributed to the incident
- Identify system vulnerabilities that enabled the incident
- Provide specific feedback to improve systems and reduce future risk
- Consider whether the incident is criminal in nature, and potentially involves engagement with law enforcement
Response

initial

- Who do they call? Set up an incident reporting hotline
- Train the first-responder(s)
  - systematic data collection and preservation
    - Get it right the first time!
  - discretion and non-provocation (!)
  - handling of sensitive information
  - event “triage”
- Route the request, as per tech assessment & priority
  - May involve calling on back-stoppers!
- Escalate, as per thresholds
  - potentially involving a national or global reporting center
Response
additional considerations

- Provide topical advice and timely assistance
  - but do not speak beyond your expertise
  - and don’t promise what you can’t deliver!
- Minimize the damage – and do no further harm!
- Preserve and protect artifacts
  - And do so in a forensically-safe manner
    - incident response will often change the state of the system, thus interfering with later analysis
- Restore systems
When an Incident is Detected …

- Do people know what to do in a crisis?
  - Would they recognize an incident when it happens?
  - Who would they contact to report or request assistance?

- Are roles defined?
  - Issues of authority, responsibility, & liability

- Do trusted relations exist?
  - Must be established in advance of actual need!

- Such questions should be asked at all levels, in advance
  - Individual
  - Organizational
  - National
General Questions re Incident Response

- Are first-responders identified and properly trained?
- Are there “default” authorized responses that can be designed in advance and rapidly deployed for different types of incidents?
  - If so, what is the “trigger” for activation?
- Are escalation procedures defined?
- Are forensically-safe mitigation and analysis methods available? And used?
- What are the respective roles and responsibilities of targeted site / ISP / CSIRT / law enforcement?
- Are there liability issues involved, regarding intervention and advice?
Sample Incident

Genericized, simplified DoS incident attack traffic, over time

Goals:
• Early detection
• Reduce impact
• Compress timeline
• Test escalation

Discover attack
Is actively monitored

Volume

Packets/sec

18:00
21:00
01:00
08:00
14:00
17:00

DDoS detected
Org Calls
National Team
• Change IP
• ISP Filter
• TCP Dump Data Collection
Start TCP dump data analysis
Apply Filtering Rules
ISP Data Collection and analysis
Post-event Review
potential aftermath questions

- When did the attack stop? When did it start?
- Was there a discernible pattern that might help future early detection strategies?
- Review the impact of mitigation strategies – what worked? What didn’t?
- Review the sequence of deploying the mitigation strategies – was order important?
- What could be done to improve detection and response?
- Was the proper escalation procedure observed?
- Were the right partners involved?
Scenario (1)

- There is a Denial-of-Service attack taking place in a neighboring country.
- The neighbor tracks a source back to your country.
- Who would they call in your country for assistance?
Scenario (2)

- There is an active Denial-of-Service attack against a major organization in your country
- You are able to trace a source back to a foreign country
- Who do you call for assistance?
The on-line payment processing web site for your organization has been compromised. Criminals have found a way to defraud the process, receiving goods and services but paying little or nothing.

It is a systemic flaw, not readily patched.

If you shut the site down, key services become unavailable.

If you continue, the fraud could increase.

Law enforcement would like the site to stay up, so as to continue the investigation.

Who makes the decision to close or stay open? Who is liable for the repercussions?
Scenario (4)

- The local newspaper has heard a rumor about your compromised payment site.
- A reporter asks you to respond for an article that will be published tomorrow.

What do you say?

- “No comment”
- “We are doing everything we can to shut this down”
- “We take all measures to protect our system”
- … or something else?
Reminders . . .

- Detect early – based on prior experience & domain exp.
- Facilitate reporting – make it easy, take it seriously
- Respond quickly, and consistently – build confidence
- Decrease the amount of time required, at every stage
- Fix the problem(s)! And prevent recurrence
- Manage sensitive information - and be discreet!
- Confidence is hard-won and easily lost
the National CSIRT model

Bank CSIRT
Ministry CSIRT
Oil co. CSIRT

Organizational CSIRTs

National Coordination Center
Government CSIRT
Sector-specific CSIRT
ISP CSIRT

• Identify Points-of-Contact
• Exchange Encryption Keys
• Establish NDAs & MoUs

Scope-of-Service
• Incident Coordination & Reporting
• Incident Analysis & Forensics
• Outreach, Awareness, & Training
• Critical Infrastructure Protection

A necessary but not sufficient component of a national cyber security strategy

Note the “CSIRTs with National Responsibility” working group
A community with complementary and reinforcing roles and responsibilities, from end-user up to the national level
Consider a set of organizations inside a country, or a group of national CSIRTs and communication amongst them.
Scaling of Points-of-Contact

... not so hard, with a handful of partners
but consider the number of bi-lateral connections ... and how it grows with each new member
... And why the use of trusted intermediaries is an appealing option

Thus the motivation for, say, national coordination or Global Response Center!
Questions?