# Security Incidents Management in EGEE

***Romain Wartel***
***Operational Security Coordination Team***
***GDB , CERN***
***4th July 2007***

# IR Policy

- **Incident Response (IR) policy**
  - **Local IR policy**

  - **"LCG/EGEE Incident Handling and Response Guide" (JSPG) Based on the Open Science Grid, Approved by WLCG Management Board on 28 Nov 2005:**

    **http://cern.ch/proj-lcg-security/docs/LCG_Incident_Response.asp**

# IR procedure for Grid hosts

**This procedure is provided for guidance only and is aimed at minimising the impact of security incidents, by encouraging post-mortem analysis and promoting cooperation between the sites. It is based on the EGEE Incident Response policy (available at https://edms.cern.ch/file/428035/LAST_RELEASED/Incident_Response_Guide.pdf) and is intended for Grid site security contacts and site administrators.**

**A security incident is the act of violating an explicit or implied security policy (ex: your local security policy, EGEE Acceptable Use Policy - https://edms.cern.ch/document/428036/3). When a security incident is suspected, the following procedure should be used:**

**1- Contact immediately your local security team and your ROC Security Contact.**

**2- In case no support is shortly available, whenever feasible and if you are sufficiently familiar with the host/service to take responsibility for this action, try to contain the incident, for instance by unplugging the network cable connected to the host. Do NOT reboot or power off the host.**

**3- Assist your local security team and your ROC Security Contact to confirm and then announce the incident to all the sites via project-egee-security-csirts@cern.ch.**

# IR procedure for Grid hosts

**4- If appropriate:**

*** report a downtime for the affected hosts on the GOCDB**

*** send an EGEE broadcast announcing the downtime for the affected hosts**

**Use "Security operations in progress" as the reason with no additional detail both for the broadcast and the GOCDB.**

**5- Perform appropriate forensics and take necessary corrective actions**

*** If needed, seek for help from your local security team or from your ROC Security Contact or from project-egee-security-support@cern.ch**

*** If relevant, send additional reports containing suspicious**

**patterns, files or evidence that may be of use to other Grid participants to project-egee-security-contacts@cern.ch. NEVER send potentially sensitive information (hosts, IP addresses, usernames)**

**without clearance from your local security team and/or your ROC Security Contact.**

**6- Coordinate with your local security team and your ROC Security Contact to send an incident closure report within 1 month following the incident, to all the sites via project-egee-security-contacts@cern.ch, including lessons learnt and resolution.**

**7- Restore the service, and if needed, send an EGEE broadcast, update the GOCDB, service documentation and procedures to prevent recurrence as necessary.**

# Security Incident prevention

***The OSCT has three main activities:***

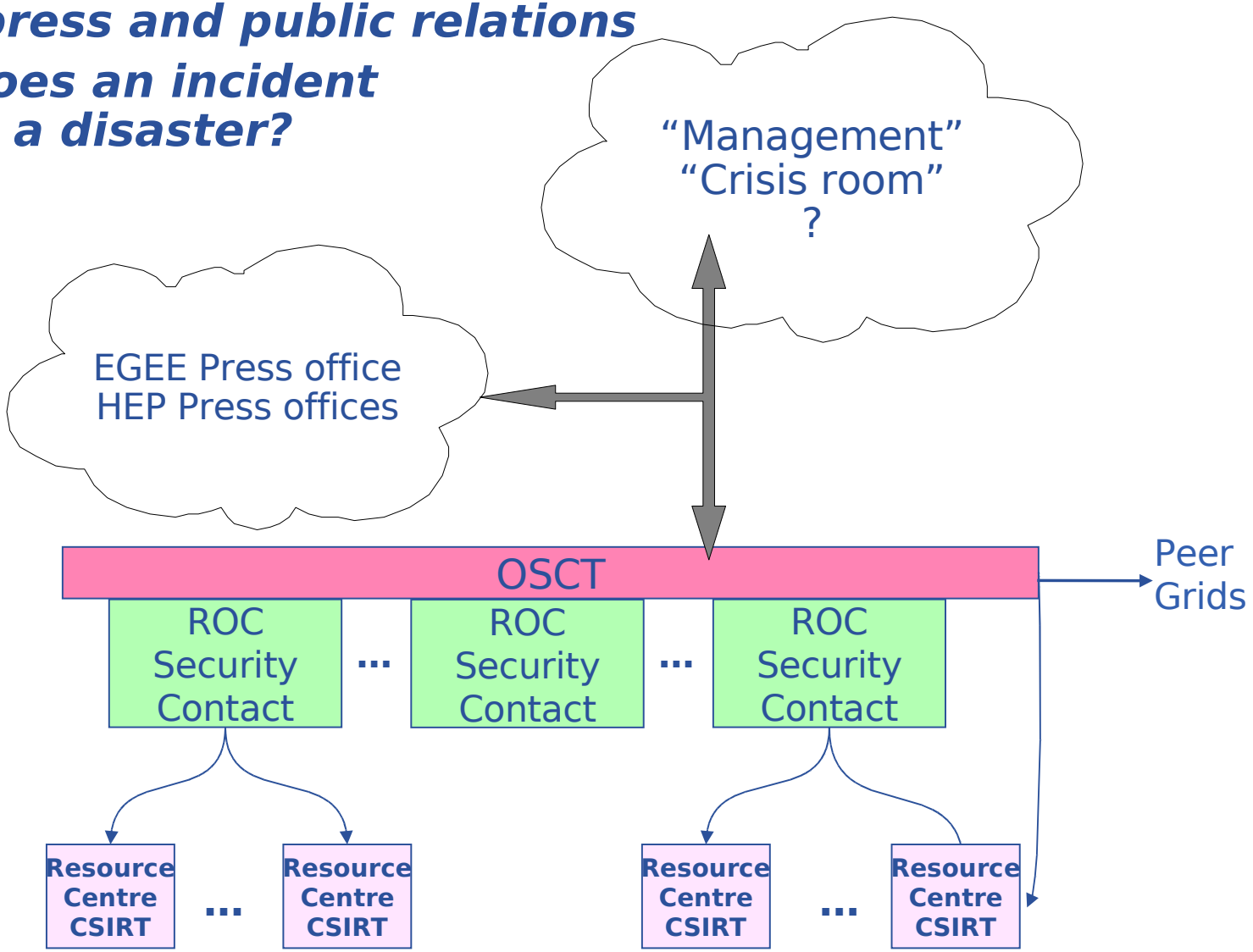
- ***Incident Response improvement***
  - ***Security service challenges (SSC) SSC1, SSC2, SSC3***
  - ***IR channels (lists, IM)***
  - ***IR Scenarios***

- ***Incident detection and containment (=monitoring)***
  - ***Several monitoring tools available to the sites***
  - ***SAM Security Tests***

- ***Incident prevention***
  - ***Best practice***
  - ***Training***

# Disaster scenarios

- ***Impact of serious security incidents on the Grid and LHC***
- ***Leaks, press and public relations***
- ***When does an incident become a disaster?***



# Main Issues

- ***Small sites vs big sites***
  - ***Incidents at big sites more spectacular and likely to attract attention***
  - ***But small sites are an easier target for attackers***
  - ***Deaths caused by sand holes (16) vs Shark Attacks (12) in the US (1990 – 2006)***
  - ***Small sites more difficult to reach (training, best practice, monitoring)***
- ***Lack of security expertise***
  - ***In the OSCT, at the ROCs***
  - ***Sites***
  - ***Developers***
  - ***VOs***
- ***Difficult to obtain promised efforts from the ROCs:***

***https://twiki.cern.ch/twiki/bin/view/LCG/PendingActions***

# Conclusion

- *IR process better understood, SSC still very useful*
- *Need to be prepared for (serious) incidents*
- *Need to identify/train management contacts for disasters*
- *We should be prepared for more sophisticated attacks, but experience shows that basic advice still need to be repeated*
- *Still a lot to do for prevention and detection, but only little progress has been made*
- *ROCs need to provide agreed efforts to make this happen*

# Teragrid incident – Press hype

*“It is unclear exactly how many systems have been compromised, but the number may be as high as 15 to 20.”*

*“Cybersecurity experts have been warning the U.S. in recent years about possible cyber attacks on sophisticated and high end computing networks. Members of al Qaeda, for instance, are known to have investigated the security of computer systems at dams, power plants and other crucial, high security facilities. [...]*

*The attackers could also use data blasts to push networks offline, much like the case in Canada where a teenager gained control of University of California, Santa Barbara computers to shut down Amazon, eBay, CNN.com and others for hours at a time.”*

*“Many institutions have applied loose security to those shared directories to "facilitate the distribution of system management and data processing tasks," the advisory said.[...]*

*it is no guarantee that the malicious hackers behind the compromise no longer have access to the sensitive networks.*

*"Once they're in a network of this size and scope, they're going to compromise other systems using stealth techniques that are different from the ones they used to get in. Once you figured out [the compromise] and know what systems are vulnerable, they're already on a different system," Bingham said. ”*

# Teragrid incident – Press hype

*“Preventable Intrusions*

*The attacks were preventable, Cooper said, if the systems had been properly patched. "I'm not aware of any new vulnerabilities being used at any of these locations [that were] anything not disclosed." The attacks were not sophisticated, he said.[...]*

*The issue is not one of cost, Cooper said, but of "poor implementation of policy and procedure."“*

*“America’s precious and powerful supercomputers are bound together by the “Grid/TeraGrid” which has now been proven to be extraordinarily vulnerable to intrusion. The recent hack of the Grid was most likely accomplished by a small group of young U.S. hackers.*

*[...]*

*Superprofessors who design supercomputers and superGrids probably hadn’t figured out what the “threat model” from hackers looks like. They probably knew they needed to keep hackers out but it appears they just didn’t figure how smart even mediocre hackers had become.”*

*http://www.stanford.edu/group/security/securecomputing/alerts/multiple-unix-6apr20(*
*http://www.computerworld.com/securitytopics/security/story/0,10801,92230,00.html*
*http://www.enterprise-security-today.com/story.xhtml?story_id=1120084PBM34*
*http://www.rawstory.com/exclusives/koch/vulnerable_computer_grid.htm*
*http://www.hpcwire.com/hpcwire/hpcwireWWW/04/0416/107444.html*