



# CERT Update

*Andy Bone*

*CERT Manager*

# Conference Admin



## **IN Case of Fire:**

**Please leave Via the exits ??????**

**Assemble in the ???????**

**Wait until directed by hotel staff.**

## **Smoking:**

**Smoking is not allowed in this conference hall.**

**Designated smoking areas are:**

**???????**

**???????**

**Please fill in the feedback form.**

**Next Conference will be in London during the first week of  
December.**



# Programme of Events.

- 0930-1000 Registration and Refreshments
- 1000-1020 Welcome and JANET-CERT Update (Andy Bone, JANET-CERT Manager)
- 1020-1045 JANET-CERT Security Situation (Mally Mclane, JANET-CERT)
- 1045-1105 Refreshments
- 1105-1205 Enterprise Firewalls (Arthur Clune, University of York)
- 1205-1315 Carvery Lunch
- 1315-1400 Indecent Images of Children on the Internet (Frank Glen, IWF)
- 1400-1445 Detection and Mitigation of DoS Attacks (Steve Mulhearn, Arbor Networks)
- 1445-1500 Refreshments
- 1500-1545 National High Tech Crime Unit (Nina Gaubert, NHTCU)
- 1545-1600 Question The Speakers and wind up session.

# Introduction



- CERT Update (Andy)
- Recent Activity (Mally)



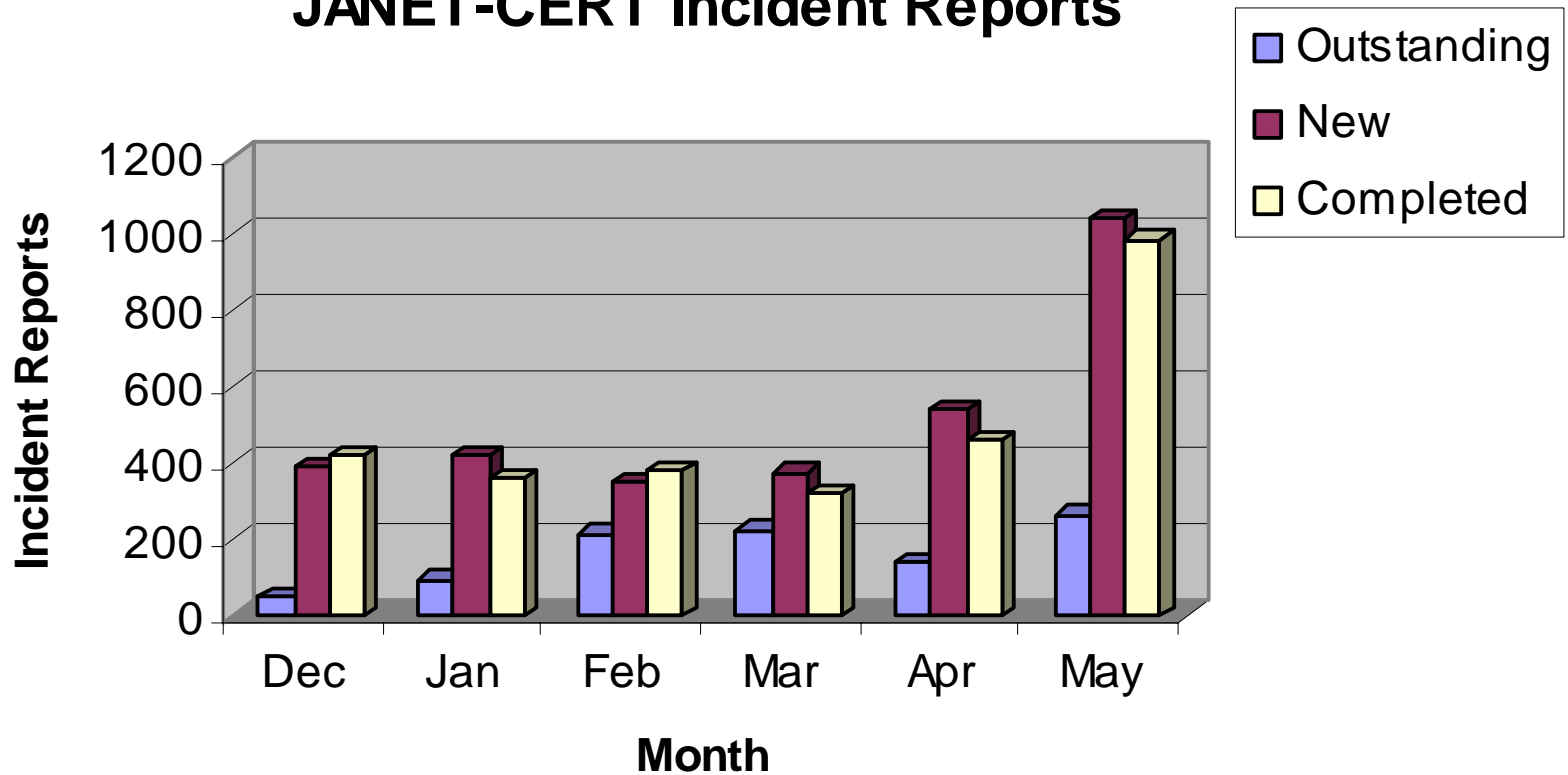
# CERT Update

*Andy Bone*

# CERT Incident Reports



## JANET-CERT Incident Reports



# Helping Us to help you



- Don't be afraid to report, we don't bite. (even if you think it's trivial it may help the larger picture)
- Please answer our mail or requests for information. (We will chase you, and keep doing so)
- If you don't understand the help or advisories we issue, please ask for clarity.
- Further Guidance for CERT contacts is on the JANET-CERT website.

# Current Projects Sept 04



- The new network has been in production since the 8<sup>th</sup> Nov 03.
- BCP will be located at Leeds testing almost complete.
- RTIR has been in production since 01 Dec 2003, some internal tweaks have been carried out. A new working group through TF-CSIRT is looking at the specification for Version 2.

<http://www.bestpractical.com/pub/rt/release/rtir.tg>

- IPHS is now in place, John will discuss later.
- Netflow, under SJ4 and SJ5, looking at different solutions.
- Website Update.
- Policy and Procedure Review.

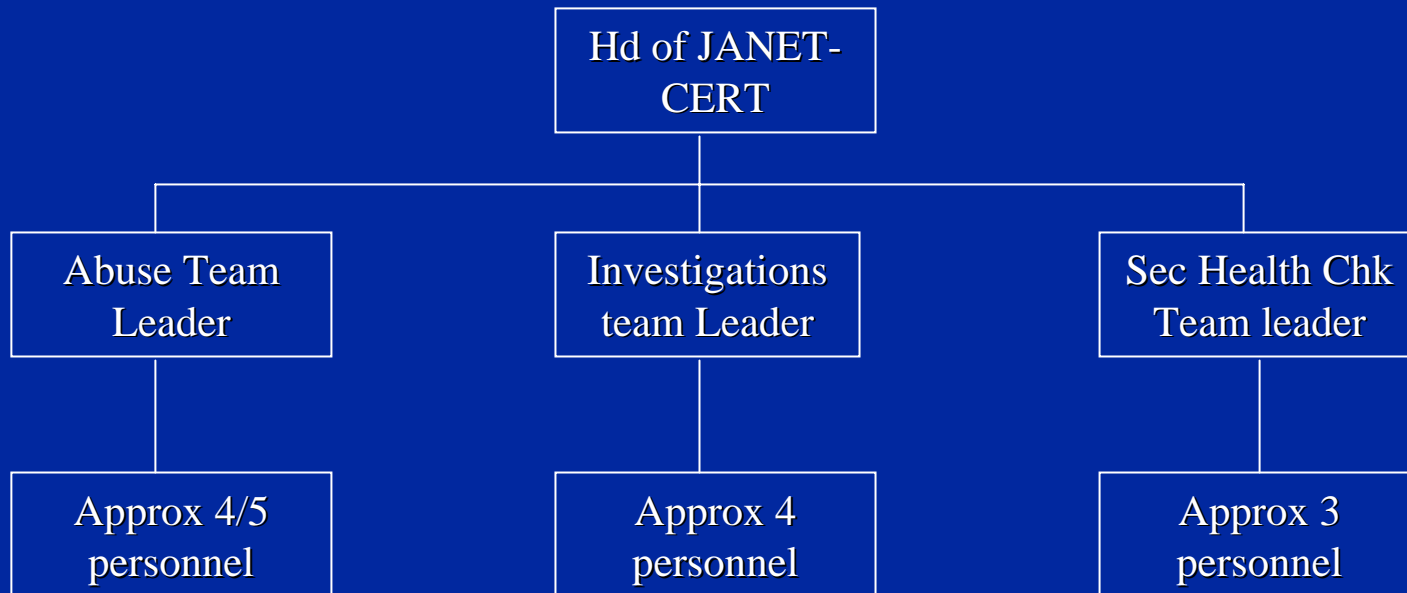


# New CERT Structure and Services

- Review of Services (the papers)
- JISC Buy in (Security within JANET).
  - Security policy framework
  - Best practice guides.
  - JANET Security Policy and AUP review.
- Proposed New Services
  - Abuse and Triage.
  - Investigations and Forensics.
  - Security Health Check and consultation.
- Team Structure.
- Time line.



# Proposed Structure



# Proposed Time Line 2004



- June, Andrew Cormack's (JANET Security Enhancement Project) paper to JCN.
- Early July, My paper to UKERNA Executive for inclusion in July JISC meeting.
- End of August, hopeful JISC agreement to proposal.
- End of October.
  - Complete and submit to the UKERNA executive and JISC the implementation plan for the new services.
  - Complete all CERT ongoing projects.
- December.
  - JISC Agreement to implementation plan.
  - Begin recruitment of service team leaders.
  - Initiate new service outlines.



# Current JANET-CERT Resources

## Staffing

- Currently 8 personnel

## Manned

- From 0800 – 1800 Mon-Fri
- Oncall 1800 – 2359 weeknights and 0900 – 1700 weekends excluding UK bank holidays, Xmas day, boxing day and Easter Sunday.

## Communications

- Email: [cert@cert.ja.net](mailto:cert@cert.ja.net)
- Telephone: +44 (0)1235 822340
- Fax: +44 (0)1235 822398



# Proposed JANET-CERT Resources

## Staffing

12/13 personnel

## Manned

From 0800 – 1800 Mon-Fri (although team oriented)  
Oncall 1800 – 0800 weeknights and 0001 – 2359  
weekends, giving 24/7 coverage.

## Communications

Possibly [abuse@ja.net](mailto:abuse@ja.net)

Email: [cert@cert.ja.net](mailto:cert@cert.ja.net)

Telephone: +44 (0)1235 822340

Fax: +44 (0)1235 822398

# Questions

