

JANET-CERT Update

John Green
Rodney Tillotson
JANET-CERT



Who

- CERT Manager
 - Andy Bone
- The Team
 - Simon Baker, Garaidh Cochrane, John Green, Tom Meyer, Robert Morgan, Rodney Tillotson, Stephen Warner-Jones
- Staff Movements
 - Andrew Cormack moved to Network Development Division



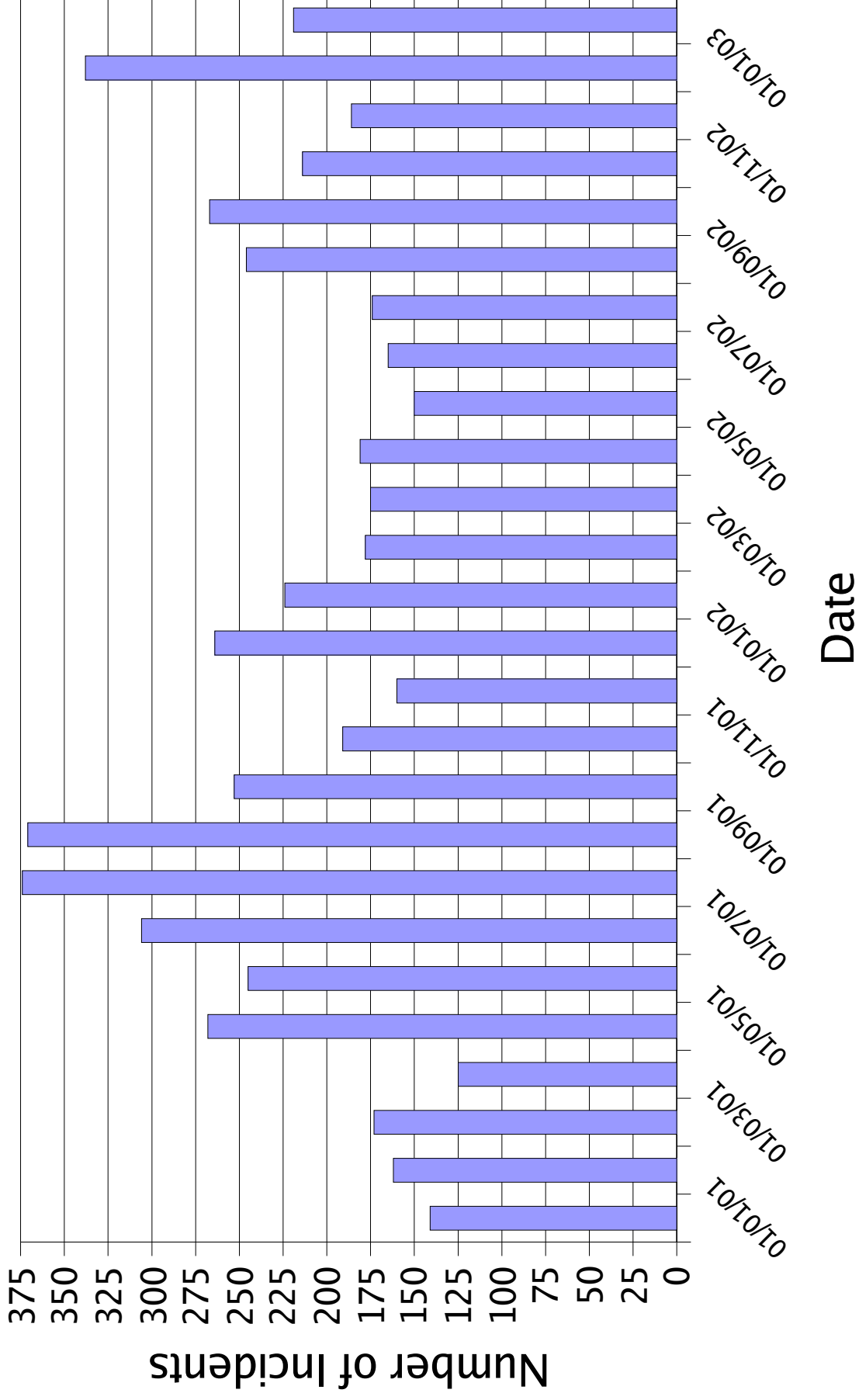
What we do

- Our SLA says
 - Incident Response
 - Provide Information
 - Raise Awareness
 - Liaison

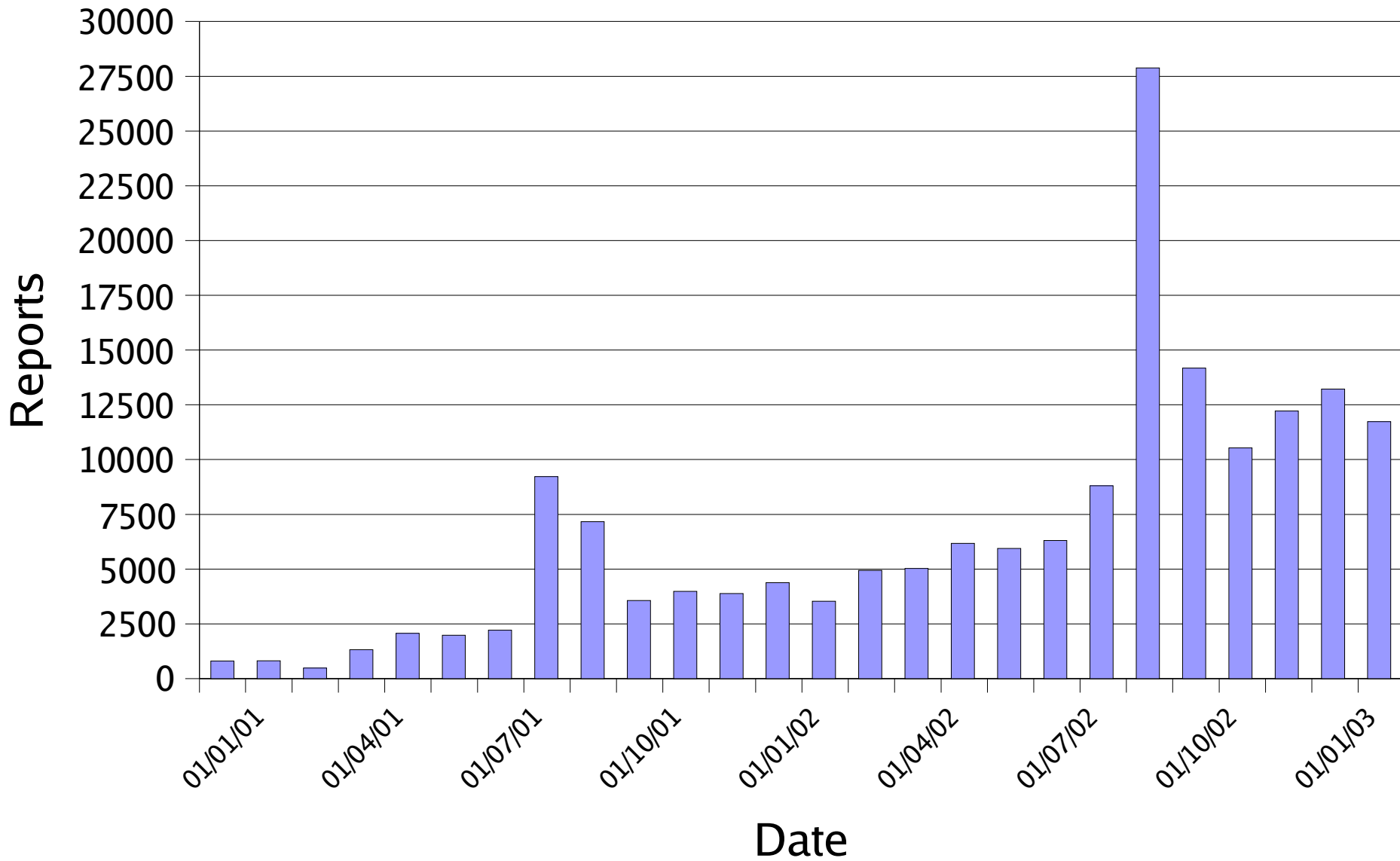
Incident Response

- Customer originated
 - Compromised machines
 - Denial of service
 - Probes (logged for information)
 - Requests for advice
- External origin
 - Scans from JANET machines
 - Open relays
 - General networks abuse (AUP)

Incidents



Informational Reports



Incident Response

- Coordinate links with law enforcement, security services
- Provide CERT service for HEANET
- Maintain contact information
- Trusted point of contact for JANET
- Protect the network

Incident Response

- Email: `cert@cert.ja.net`
- PGP ID: `0x836D7141`
- Phone: `01235 822340`
- Fax: `01235 822398`
- Service hours: `8am-6pm weekdays`
- Oncall: `6pm-midnight weekdays`
`9am-6pm weekends`



How you can help

- Answer emails promptly, so we know an issue is being dealt with
- Keep contact information up to date
 - Email service@janet.ac.uk (JCS)
- Feel free to report unusual events
 - Probes/scans (with prior arrangement)
 - System compromises using new vulnerabilities
 - Interesting code or log entries left on machines
In particular those which implicate JANET hosts!



Information

- Maintain the uk-security mailing list
 - uk-security for general discussion
 - uk-security-announce for announcements
- Significant alerts sent to list
 - New threats (eg SQL Slammer)
 - General advice to whole community
- Forum for discussion within ac.uk

Information

- Website
 - Links to useful sites, tools, checklists
 - Contact information
 - Advice on computer security
 - Legislation (RIPA, Data Protection)
- *Content to be reviewed over the coming months*

Awareness

- Contribute to the Security course provided by UKERNA
- Course currently being revised into two separate courses
- Give presentations to
 - RSCs
 - JANET user groups
 - Networkshop



Liaison

- Participate in
 - FIRST (Forum for Incident Response and Security Teams)
 - TF-CSIRT (TERENA Task Force)
 - Trusted Introducer
 - UKCERT
 - RIPE

New Developments

- Current system lacked scalability to cope with increasing number of incidents
- New system in development based on ticketing system Request Tracker
- Customised to
 - Map onto Incident Handling workflow
 - Manage hierarchical form of security incidents
 - Access our other data sources (eg contacts)

New Developments

- Plans for system to ease analysis of probe information
- Allows new threats to be observed quickly
- Unusual traffic flows can alert us to compromised machines on network
- Possibly incorporating netflow information

ECSIRT.net

- European funded project to develop tools to facilitate CSIRT->CSIRT communication
- Working with a number of European NRN CSIRTs
- Involved in IETF INCH-WG designing common-language (IODEF)
- Project due to complete early 2004



What we **don't** do

- Secure your systems
- Manage the routers
- Penetration testing
- System Admin support
- Abuse desk
- Talk to end-users

Feedback

- What do we do that you like?
- What do you do that you dislike?
- How could we do things better?
- What services would you like us to offer?

Code Red days

- Freak occurrence
- 100's of infected machines on JANET
- Several at some sites
- Top priority is the network
- Need prompt replies from sites
- Mopping up can take weeks