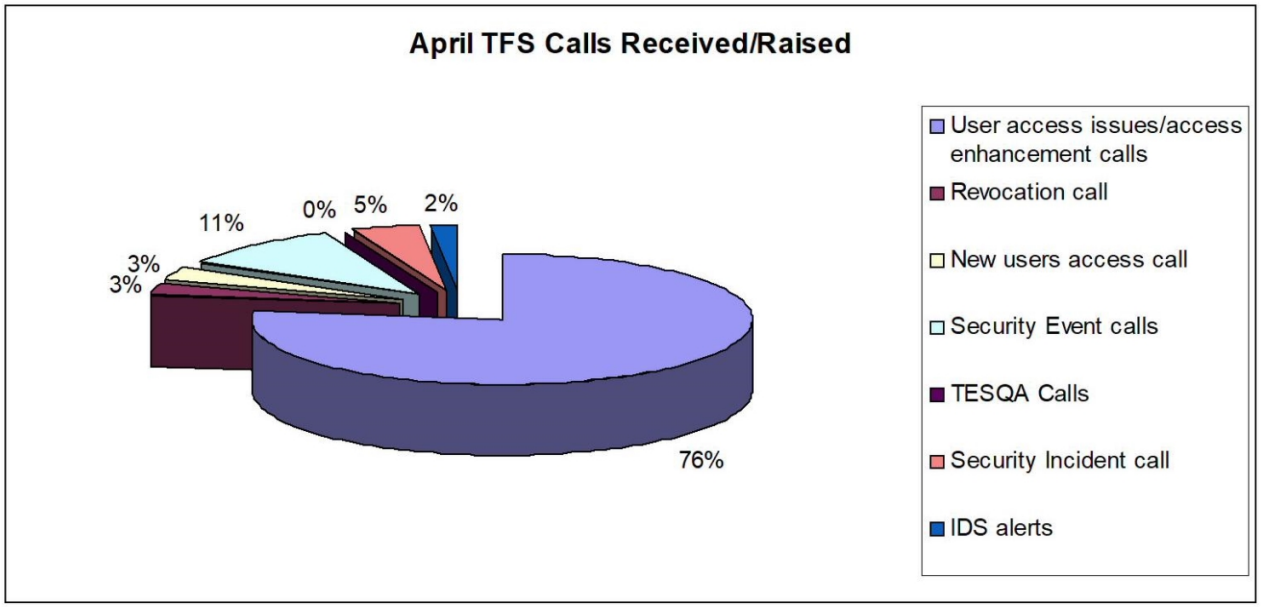
FUJ00231986

RMG Security Ops Service Management Report

Monthly Review – April 2011

SECURITY INCIDENT MANAGEMENT – TFS and PEAK

FUJ00231986



TFS - 'A' Priority calls raised/ handled this month:-

Call Reference No:	Date Opened	Days Closed	Summary	RAG
			N/A	

PEAK 'A' Priority calls raised on the Security Ops stack:-

Call Reference No:	Date Opened	Days Closed	Summary	RAG
PC0205980	**1 Nov 10**		**LST: Sophos Anti virus is quarantining files**	

FUJ00231986

USER ACCESS MANAGEMENT

Area under construction – example of what we expect to show start new financial year

Total number of users with System access = 272

New Joiners for April - 2
Leavers/revocation for April – 2

User Management	Revocations – Access removed within 24 hours of receipt of call/form (G = 90 -100% , A = 70 – 80%, Red= 70% &<)		
	New User access – Setting up of MSAD Accounts within 3 days of receipt of call/form (G = 100% , A = 90+ A% - 120, R = Anything else)		

TESQA

Total accounts available to POL users – 20

Active POL accounts – 17

Unassigned/Available POL accounts - 3

Engineers – Security Clearance

254 Security Cleared Engineers.

Summary:

8 WIP currently with POL awaiting Security Clearance – (Mark Hall/David Hawkins/Ashley Jones-Mayne/Graham David-Allen/Walid Hamid-Adam/Philip Skillen/Mark Truss/Anthony Isherwood).

FUJ00231986

SECURITY KEY MANAGEMENT

Total number of cryptographic Keys Managed

Service Effect = 8
Non Service Effecting = 14
Change on compromise only = 6

Crypto Key Activities	Required key changes are taking place or scheduled to take place in the agreed timescales as per the key change schedule or as per customer request. (G = All on schedule, A = Some not on schedule, but not service affecting, R = Anything else)		Periodically

Summary:

FUJ00231986

SECURITY PATCH MANAGEMENT

Security Patching	Critical Patch deployment success rate – PAB defined (G = 100% , A = >45 days, Red= >60 days)	N/A	Within 30 days
	Patch deployment success rate within agreed timescales – PAB required (G = 100% , A = 90+ A% - 120, R = Anything else)		Within 90 days

Summary:

April patches for deployment

Microsoft released – 17 patches released – 13 require deployment
Redhat Released - 2 patches both applicable
Solaris Released - 24 patches - 13 deemed applicable

Deployment scheduled for weekend of the 05 June 2011

ANTI-VIRUS MANAGEMENT

Virus Attacks

No reported attacks

Mal-ware updates (AV)	Weekly Anti-virus definitions deployed to all the windows based platforms within 7 days of package release date (G = <7days, A = 8-13days, Red = 14& >days		Packaged Weekly on a Wednesday

Summary:

FUJ00231986

SECURITY EVENT MANAGEMENT

Security Events Received

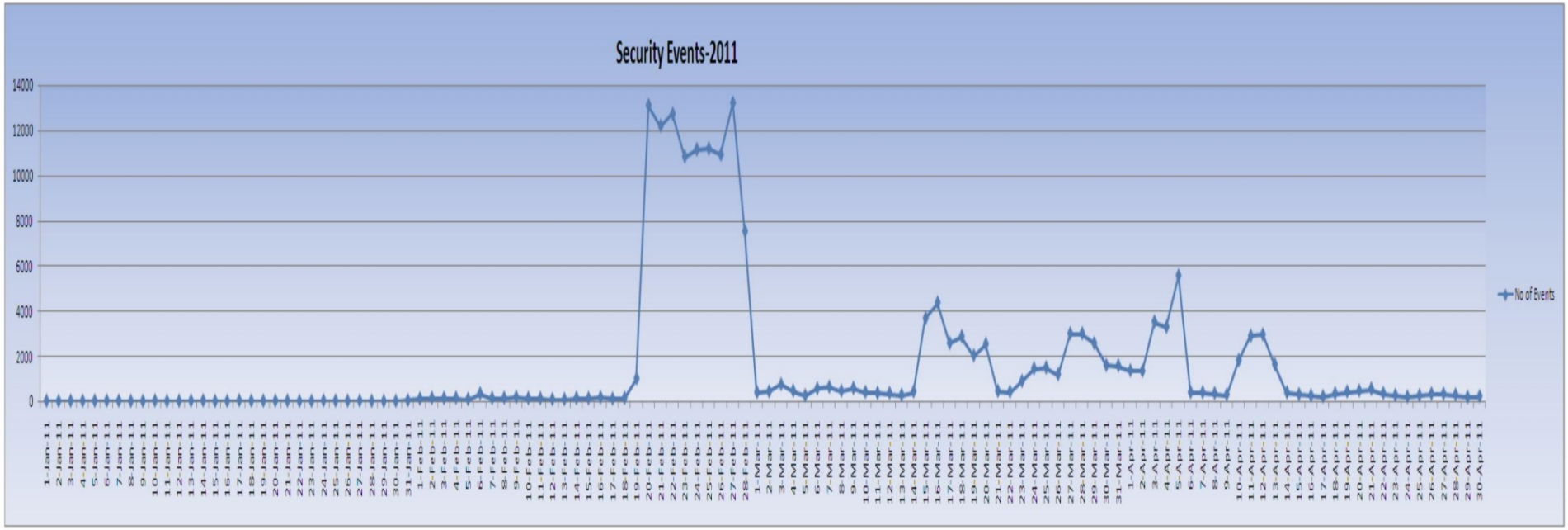
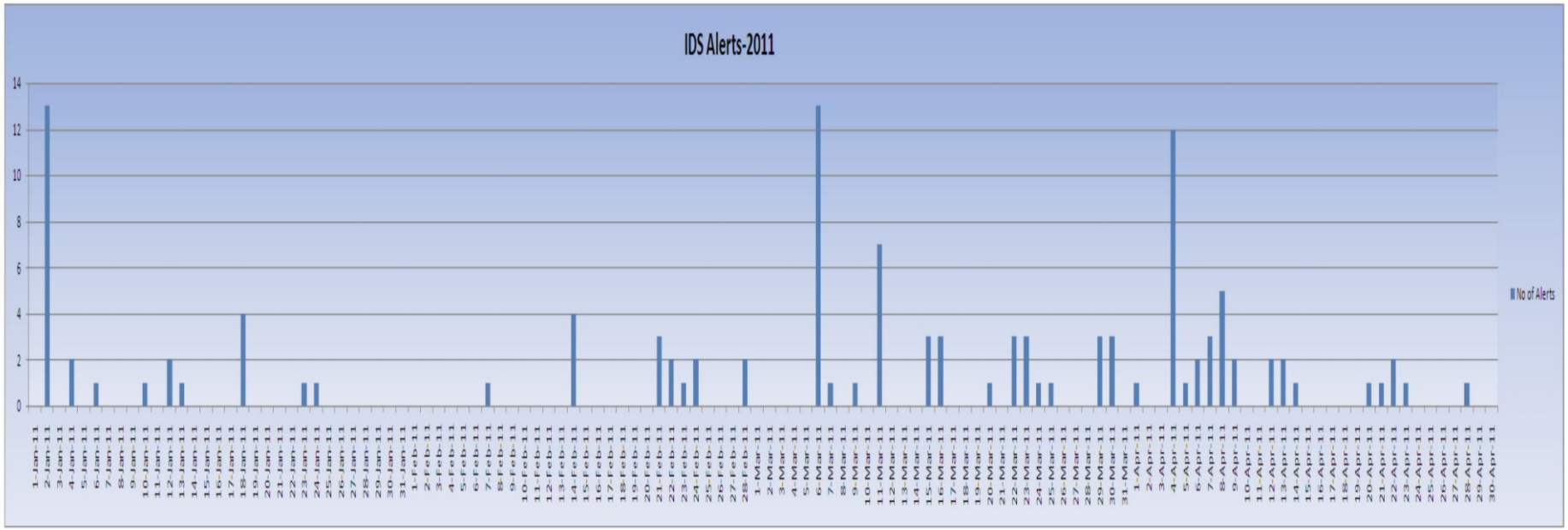


Chart 1 - Ongoing

Summary: 4 unknown events and 2 known event calls were raised during this month.

IDS MANAGEMENT

FUJ00231986



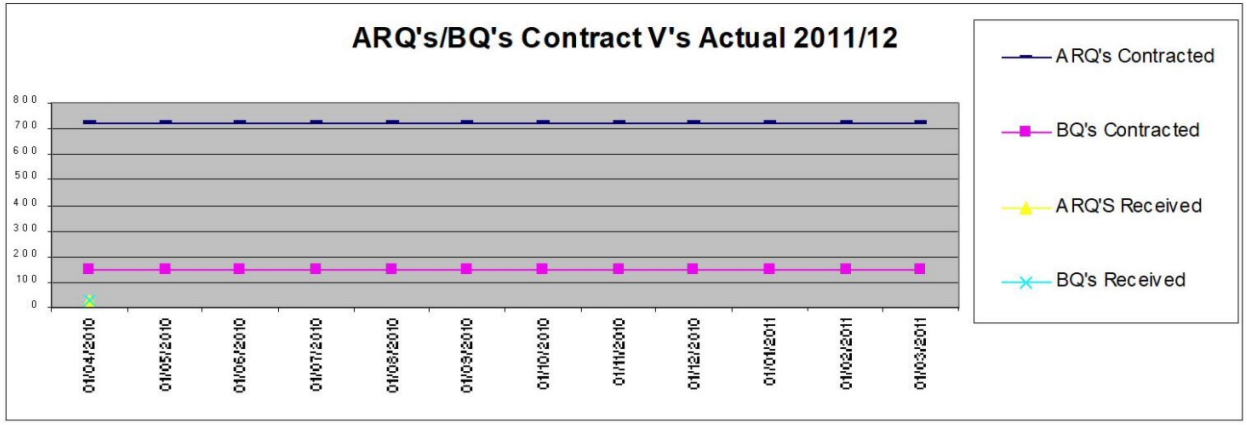
Work is in progress for additional reporting for this area and will be available in May's report.

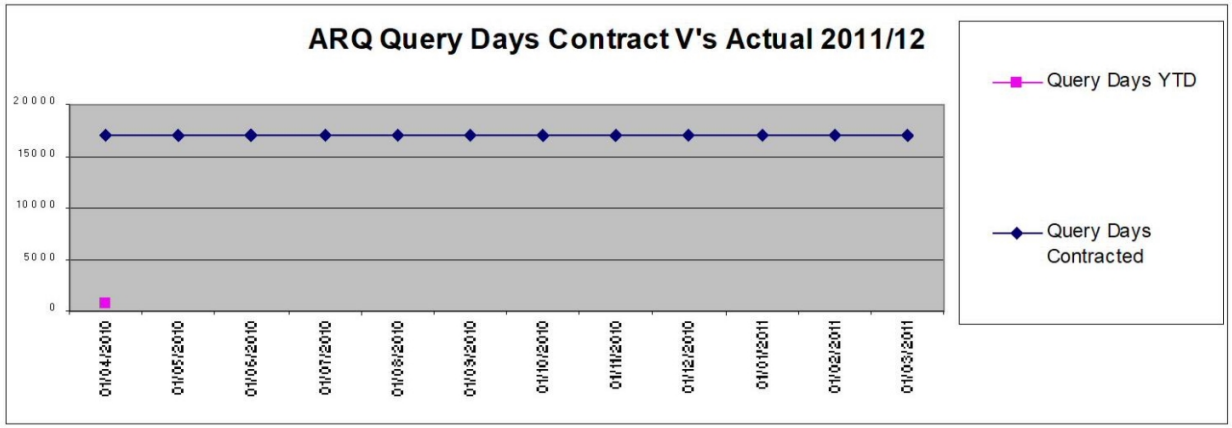
Summary:
It has been agreed that we will only be monitoring and reporting on alerts/attacks classified as High.

One IDS Call was suspended last month and is currently under investigation. Awaiting response from Jason Clark. Call Ref: 3404183.

FUJ00231986

LITIGATION SUPPORT SERVICE





Summary: CP to change the service deliverables has been agreed for 2011/2012

FUJ00231986

FIREWALL SECURITY MONTHLY REPORT

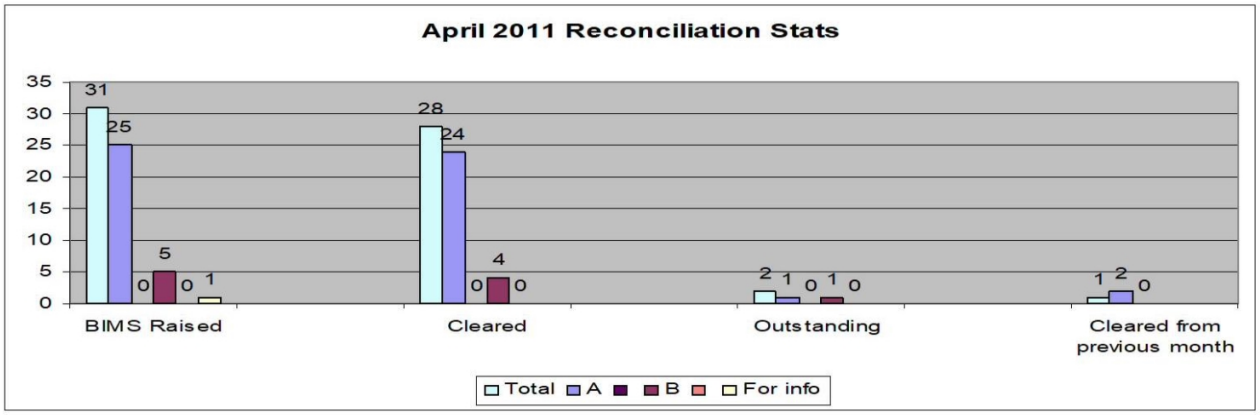
For Month Ending: 31st March 2011

This area is under review – discussion underway re what changes or additional reporting can be made available

REPORT	*Signature*	*RAG*
Any incidents of downtime on any of the Firewall's this month if so what and why.	***TIM ROPER***	
Any known unauthorised access to any of the Firewall's this month if so who and why.	***TIM ROPER***	
Any unauthorised changes to the rule-base /config or IOS upgrades this month if so when & by whom.	***TIM ROPER***	
Number of timeout issues or bad packet errors (runts/giants/CRC etc) experienced this month.	***TIM ROPER***	
Number of translation errors occurred this month for NAT/PAT if so what and why.	***TIM ROPER***	

FUJ00231986

RECONCILIATION SERVICE



BIMS Reference	Exception Type	Date Received	Suspended Date	SLA Type	Root Cause	Suspension Confirmation	Date Cleared?
0209612	EPOSS/POLFS	13/04/2011	13/04/2011	5 day SLA	Waiting for receipts of transaction Comms issue at branch unable to progress this until comms has been resolved	Mark Wardle	
0209773	LINK State 4	18/04/2011	18/04/2011	8 Hour SLA		Mark Wardle	

Summary: 31 BIMs (Business Incident Management) were issued during April, 25 BIMS were 'A' priority calls, 5 'B' priority calls and an additional call was raised for Info purposes to POL. 2 BIMs are currently outstanding these have been suspended as agreed with Mark Wardle. **All BIMS raised and cleared during month of April met SLA**.

FUJ00231986

SERVICE IMPROVEMENT PLAN

Improvement Initiative	Benefit / Outcome	Estimated Timeframes	Status
New business activities/improvements	Produce plan to facilitate POL's FoOG activities – joint activity		Apr – Discussion to held in ISMF and monthly catch up sessions
Review of the AV strategic approach	Slicker process	Apr 2011	Dec Internal Scoping CP to be raised by end Jan Jan – Meeting held with Sophos and areas of improvement under discussion Feb – CP raised for impacting Mar – CP with Chief Architect Apr – under review
Tripwire baselining	Policies being reviewed to monitor the relevant files rather than all.	June 2011	Work underway Nov – Baselining work 85% completed and documentation underway, knowledge transfer scheduled for early December for Unix and Wintel resource Dec – knowledge transfer complete scoping CP raised to understand service impact Jan – CP out for impacting Mar – Meeting scheduled for 26/04 Apr – Meeting held, follow up to be scheduled Mid May
Re work of Security operations forward Schedule of change	Clear view for all to see any changes/audits etc	ongoing	Nov – under review Dec – format changed, work still on going Mar – Audit dates to be added