

Know Yourself

GridPP Tier2 Site Security Review

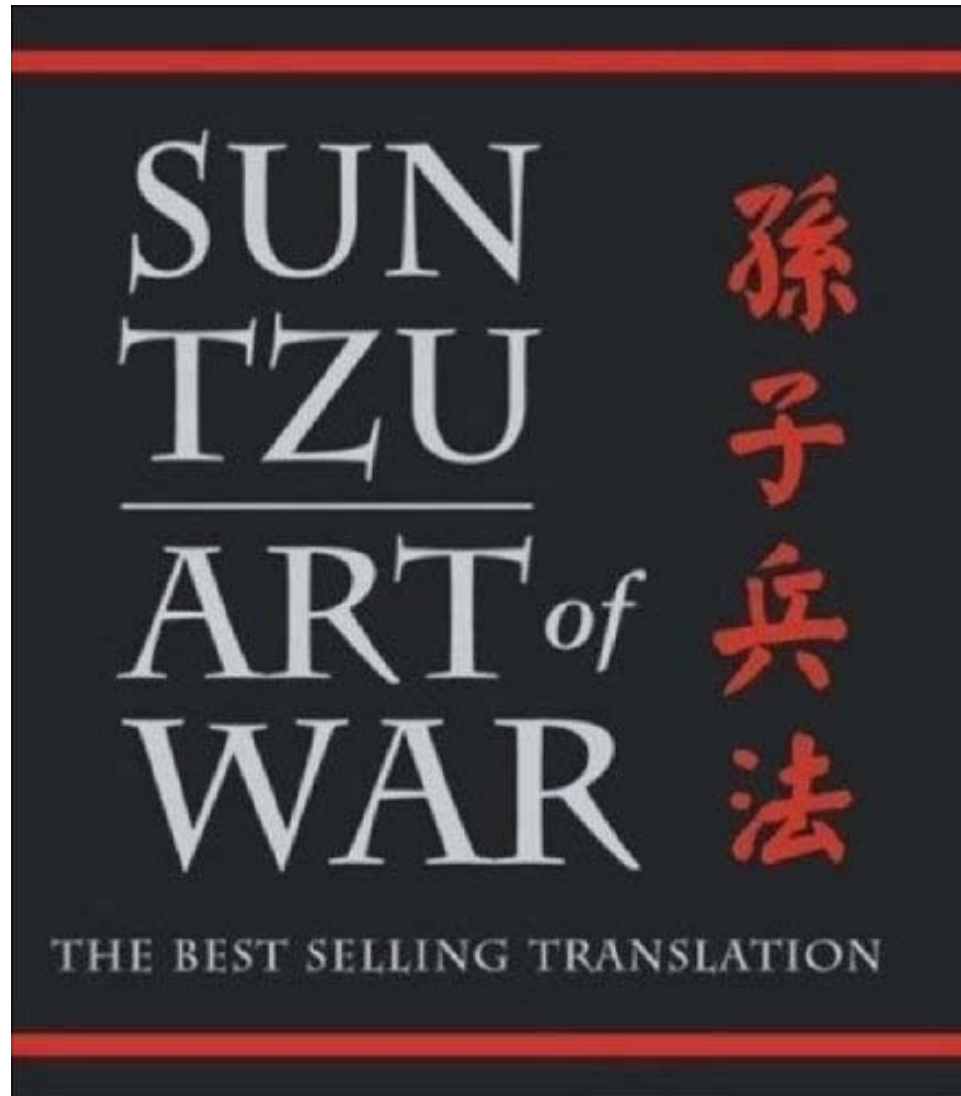
Mingchao Ma

STFC - RAL

GridPP24, 15th April 2010

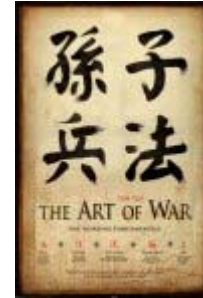


Sun Tzu:
Ancient Chinese
military
strategist and
tactician



知己知彼， 百战不殆！

《孙子·谋攻篇》



Know your enemies and know yourself,
You can win a hundred battles without a
single loss.

The Art of War by Sun Tzu

Know Yourself!

Do you?

The enemy





Advertisement

Citibank® Savings Plus Account

1.01%
APY*

For balances of \$25,000 or more.

A
a

Money » Personal Finance ■ Taxes ■ Retirement ■ Mortgage/CD Rates ■ Stock/Fund/

GET A QUOTE: GO ■ DJIA 10,306.22 ▼ -77.16 ■ NASDAQ 2,213

NEWS POLITICS OPINIONS BUSINESS LOCAL SPORTS ARTS

SEARCH: go | Search Archiv

washingtonpost.com > Technology > Security Fix



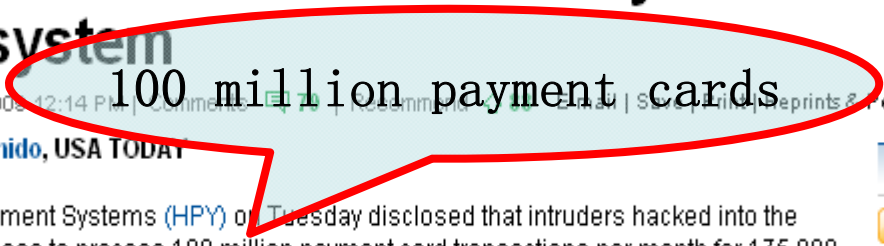
About This Blog | Archives | Security Fix Live: Web Chats | E-Mail Bri

SEARCH THIS BLOG

Go

- RECENT POSTS
- E-Banking on a Locked Down PC, Part II
 - ChoicePoint Breach Exposed 13,750 Consumer Records
 - President Obama on Cyber Security Awareness
 - Mozilla Disables

Hackers breach Heartland Payment credit card system



Updated 1/23/2008 12:14 PM | Comments (17) | News Alerts | Search | Site Map | Reprints & Permissions |

By Byron Acohido, USA TODAY

Heartland Payment Systems (HPY) on Tuesday disclosed that intruders hacked into the computers it uses to process 100 million payment card transactions per month for 175,000 merchants.

Robert Baldwin, Heartland's president and CFO, said in a USA TODAY interview that the intruders had access to Heartland's system for "longer than weeks" in late 2008. The number of victims is unknown. "We just don't have the information right now," Baldwin said.

Tech security experts said the breach could set a record. Retail giant TJX lost 94 million customer records to hackers in 2007. With more than 100 million transactions per month, they could discover that several months' worth of transactions were captured, says Michael Maloof, chief technology officer at TriGeo Network Security.

Hackers Break Into Virgin Database, Demand Ransom

Hackers last week broke into a Virgin pharmacists to track prescription drug more than 8 million patients and request ransom note demanding \$10 million according to a posting on Wikileaks leaked documents.

Wikileaks reports that the Web site for the Virginia Prescription Monitoring Program was defaced last week with a message claiming that the database of prescriptions had been bundled into an encrypted, password-protected file.

- Share
- Yahoo!
 - Add to M
 - Facebook
 - Twitter
 - More
 - Subscribe
 - myYahoo!

Organized Crime, after big money!

GST

GREEK SECURITY TEAM

10/09/08 03:00

Αυτήν την ώρα γίνεται η απόπειρα πειράματος στο CERN.

Ο λόγος που διαλέξαμε αυτή τη σελίδα είναι για να σας θυμίζουμε μερικά πράγματα.

Δεν έγινε βάση κάποιας προσωπικής μας αντιπαράθεσης με την ομάδα διαχείρισης του CERN αλλά με βάση την μεγάλη επισκεψιμότητα που θα αποκτήσει τα επόμενα 24ωρα ο συγκεκριμένος διαδικτυακός τόπος λόγω του πειράματος.

Μερικά στοιχεία απ' τη βάση :

```

      USERNAME USER_ID CREATED
      SYS 0 2008-02-18 16:19:25.0
      SYSTEM 5 2008-02-18 16:19:25.0
      OUTLN 11 2008-02-18 16:19:28.0
      DIP 19 2008-02-18 16:21:17.0
      TSMSYS 21 2008-02-18 16:23:27.0
      DBSNMP 24 2008-02-18 16:24:25.0
      WMSYS 25 2008-02-18 16:24:53.0
      EXFSYS 34 2008-02-18 16:27:55.0
      XDB 35 2008-02-18 16:28:04.0
      PDB_ADMIN 46 2008-02-18 17:26:32.0
      GLEGE 49 2008-02-19 10:13:07.0
      PDBMON 45 2008-02-18 17:25:24.0
      BALYS 44 2008-02-18 17:25:24.0
      USERMON 48 2008-02-18 17:59:26.0
      ..etc...etc...
  
```




Hello,

Due to our new security update and removal of all unused accounts you will have to confirm your e-mail by signing into your account. We would also be shutting down all unused accounts.

What you need to do:

1. Log in to your account at <https://webmail.uea.ac.uk/squirrelmail/src/login.php>, by clicking the URL.
2. Enter your user ID and Password.
3. Once you log in a new security profile would be updated for your account.

After following the instructions in the letter, your account will not be interrupted and will continue as normal. Thanks for your attention to this request. We apologize for any inconvenience.

Please log in to your account immediately and continue to use the account as normal while enjoying our new security updates.

<https://webmail.uea.ac.uk/squirrelmail/src/login.php>

Webmaster.

<https://webmail.uea.ac.uk/squirrelmail/src/login.php>

uea.ac.uk https://webmail.uea.ac.uk/squirrelmail/src/login.php

Google 字典 RAL OSCT EGEE GridPP NGS Information Security EGEE Security Training

University of East Anglia - Login University of East Anglia - Lo... Tari Tour -



University of East Anglia Login

Username:

Password:

Login



University of East Anglia Login

Username:

Password:

Login

BBC NEWS

UK climate unit's e-mails hacked

The e-mail system of one of the world's leading climate research units has been breached by hackers.

E-mails reportedly from the University of East Anglia's Climatic Research Unit (CRU), including personal exchanges, appeared on the internet on Thursday.

A university spokesman confirmed that information was taken and published.

An investigation was underway and

"We are aware that information from one area of the university has been," a spokesman stated.

BBC NEWS

Climate science 'openness' urged

By Roger Harrabin
Environment analyst, BBC News

MPs investigating the climate change row at the UK's University of East Anglia (UEA) have demanded greater transparency from climate scientists.

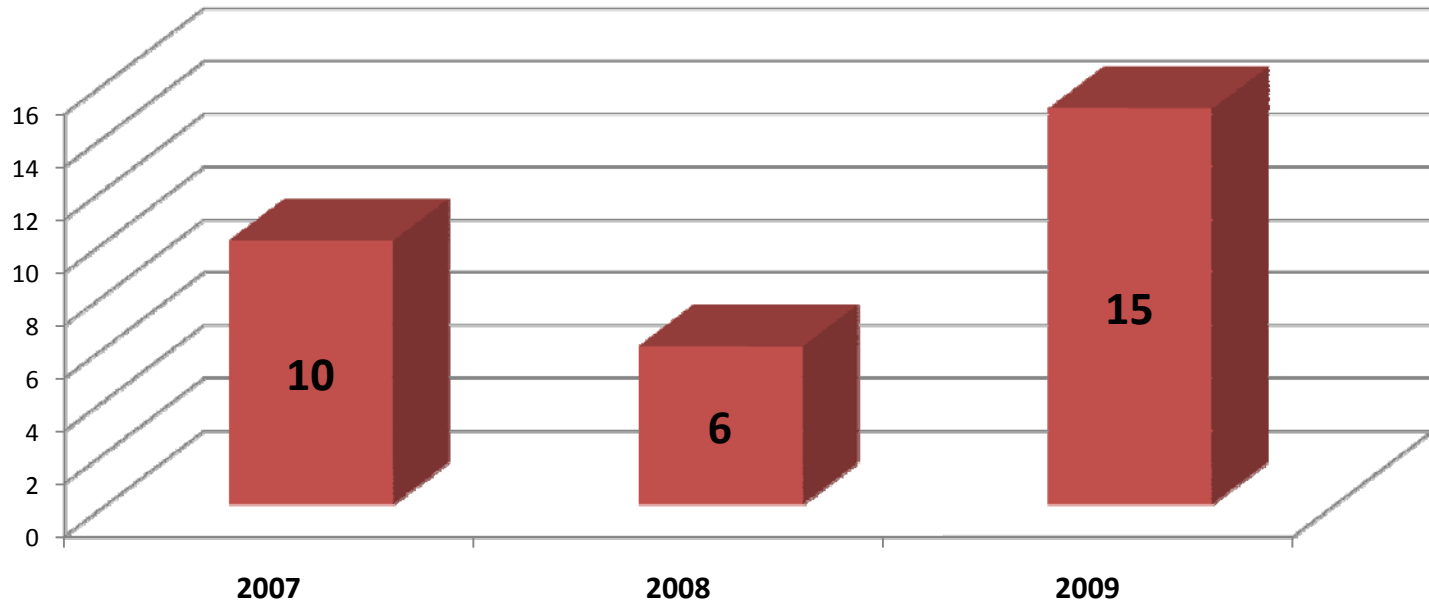
The Commons Science and Technology Committee criticised UEA authorities for failing to respond to requests for data from climate change sceptics.

But it found no evidence Professor Phil Jones, whose e-mails were hacked and published online, had manipulated data.

It said his reputation, and that of his climate research unit, remained intact.

Reported Incidents in EGEE/WLCG

EGEE/WLCG Security Incidents



- 2008, 2 incidents involved GridPP sites
- 2009, 1 incident involved GridPP sites

Know Yourself

Site Security Review

Thanks for your effort and time to
complete the questionnaire!

Objective

- “This review is aiming to have an **overview** of individual site security posture and an **overall picture** across the whole GridPP project. The output of this review will assist GridPP project to improve overall security and will also help the project make a medium and long term plan of security improvement.”

Scope

- “This review only concentrates on the fields of **operational security** such as security incident handling, patch management and log management ...”
- “... It is not intended to be a comprehensive security audit ...”

The Number

- All tier2 sites (20)+ GridIreland
- RAL Tier1 is not included

The Review

- Security policy
 - 7 questions
- Security incident management
 - 9 questions
- Logging and log management
 - 10 questions
- Patch management
 - 4 questions
- Security monitoring & protection
 - 8 questions

Overall Comment

“This security review must be considered as very much welcome. Most of those questions should be presented to any system administrator in his/her first months of work in the grid. However, it is worth to point that a questionnaire can only be a first step in improving security.”



Another Comment

“For understaffed sites, this is yet more oppressive administrative work. Lots of probing questions.”



One More

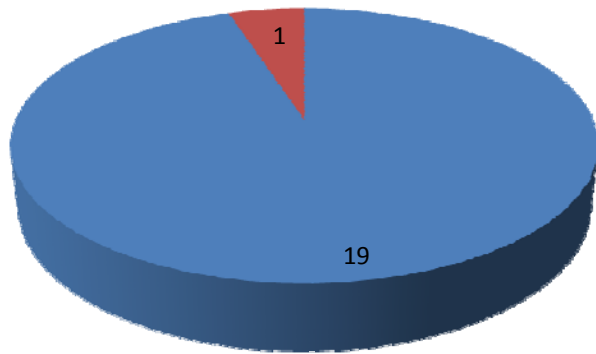
- “... We have not answered some questions in this survey because they conflict with our policy of not exposing details about our security procedures. However, we satisfy all GridPP security policies.”



Security Policy

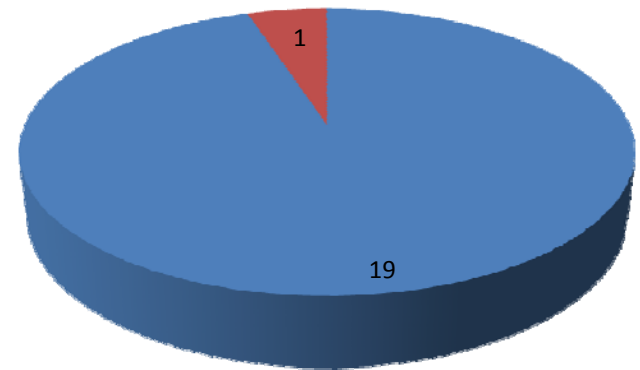
- Aware of both local (university) security policies and GridPP/EGEE security policies?
- Compliance with security policies?

Security Policy Awareness



■ Yes ■ Partially

Security Policy Compliance



■ Yes ■ Partially

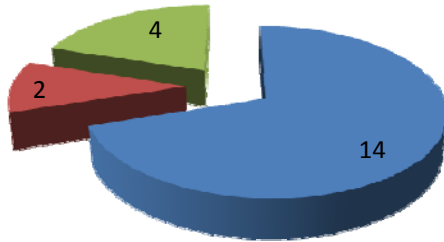
- Good awareness
- However, discrepancy on policy compliance/enforcement

Security Incident Management

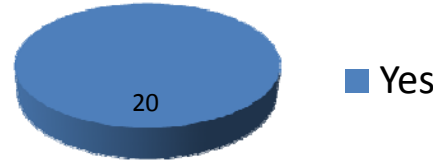
- A documented LOCAL incident handling procedure?
- Aware of GridPP/EGEE incident handling procedure?
- Appointed security officer/security contact?
- How to handle an incident?

Awareness of EGEE/GridPP Procedure

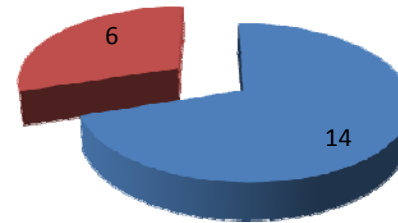
Local Incident Handling Procedure



■ undocumented/ad-hoc ■ Being documented
■ documented



Appointed Security Officer/Contact



■ Yes
■ No

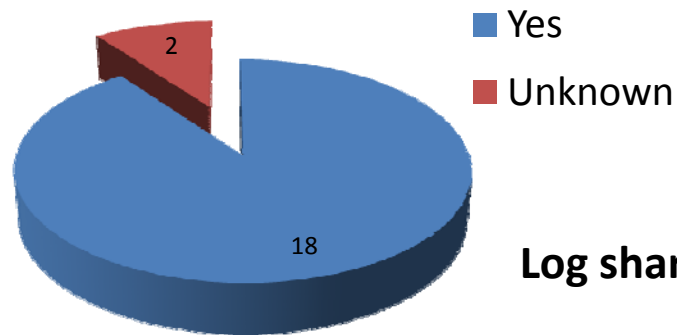
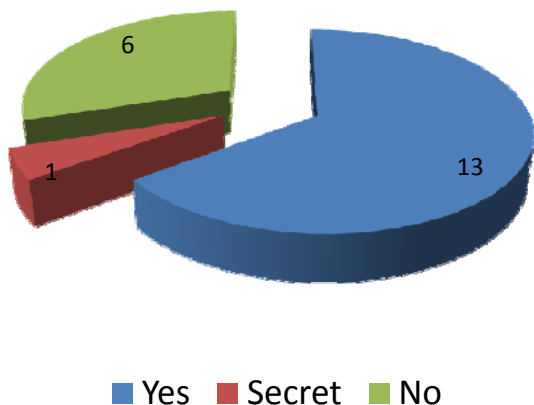
- Good awareness of incident handling procedures
- But, incident handled in ad-hoc manner at most sites

Log Management

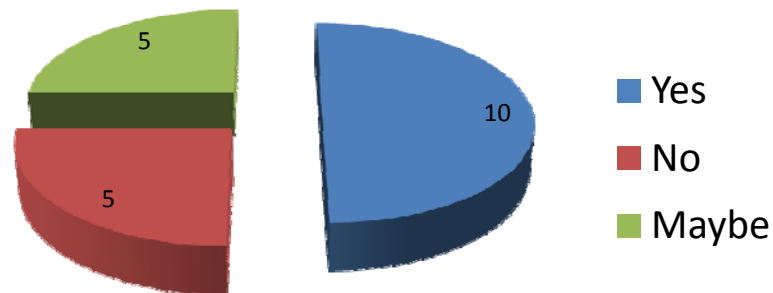
- Central logging facilities?
- Log rotation compliance?
- Log sharing across GridPP sites?
- How is log managed at site?
- Periodically log/security review?

Log Rotation Compliance

Central logging facilities



Log sharing

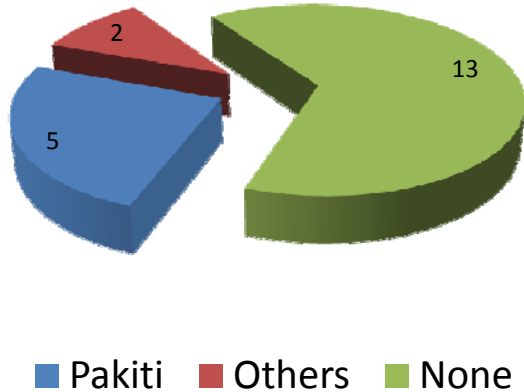


- “The logs **MUST** be collected centrally at the service provider level.”
- “**MUST** be retained for a minimum of **90** days. Grid Security Operations **MAY** define longer periods of retention”
- **6 months** prior to the discovery of the incident for successful SSH connections against grid services, and for the originating submission host for grid jobs

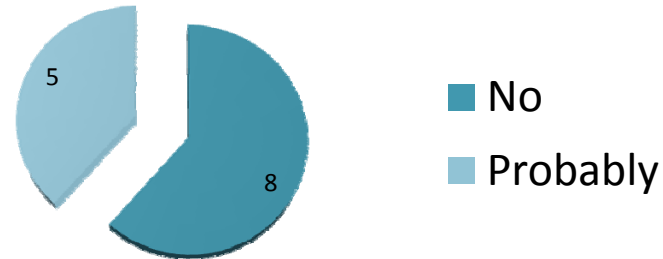
Patch Management

- Patch management system deployment?
 - NOT a package management system
- Patching procedure?

Patch Management System



Consider deploying one

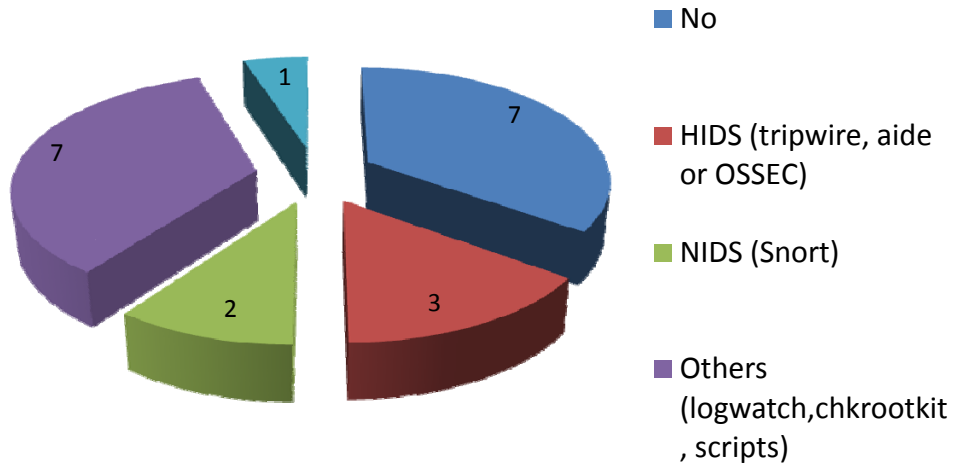


- Package management system and configuration tools
- Pakiti is complementary to above tools
- Most sites do not have documented patching procedures

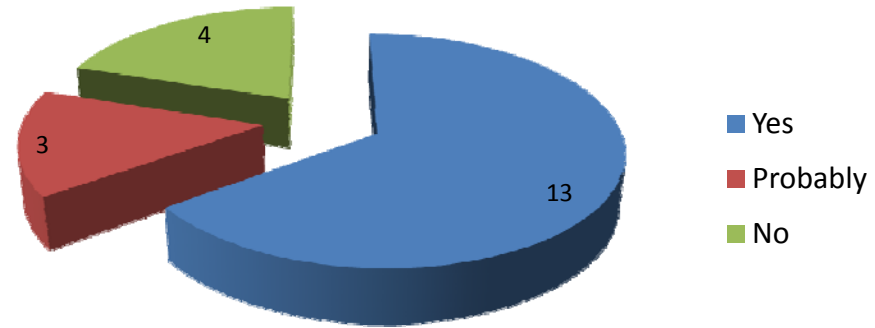
Security Monitoring & Protection

- Any IDS system?
- How to handle security alerts?
- Firewall?

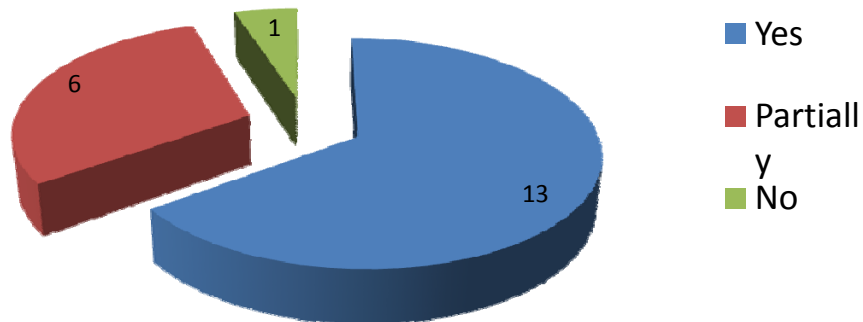
Site Security Monitoring Tool



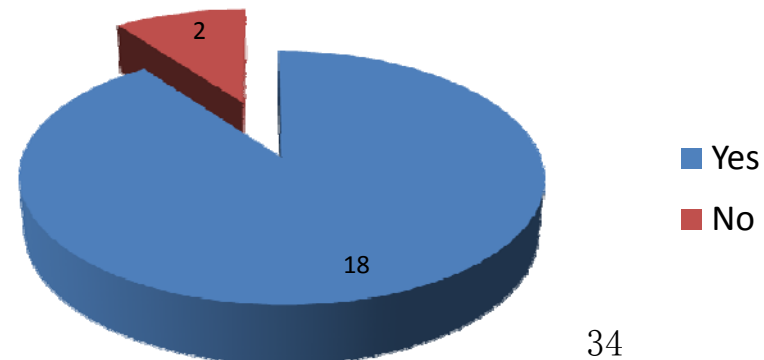
University Network Monitoring Tool



Tier2 Site Firewall



University Firewall



- Most sites have no or very basic/rudimentary monitoring tools
- Room for improvement in Firewall
- Make the most use of university' s tools if there is one

Site Concerns

- Lack of resources
 - Staff & Hardware
- Lack of security training

Observations

- Good security awareness
- Common understanding
 - Security is important
- Fire fighting style
 - Undocumented/ad-hoc
- Lack of security monitoring tools in general
- Lack of central logger somehow worrying
- More effort/resources required

Thank You!

- <https://www.gridpp.ac.uk/security/review/answers/list.html>
- Subject to access control
- Only PMB member can view them, but can open to all sites if no objection
- A summary will be available online as well
 - <http://www.gridpp.ac.uk/security/review/index.html>

Do you know yourself?

