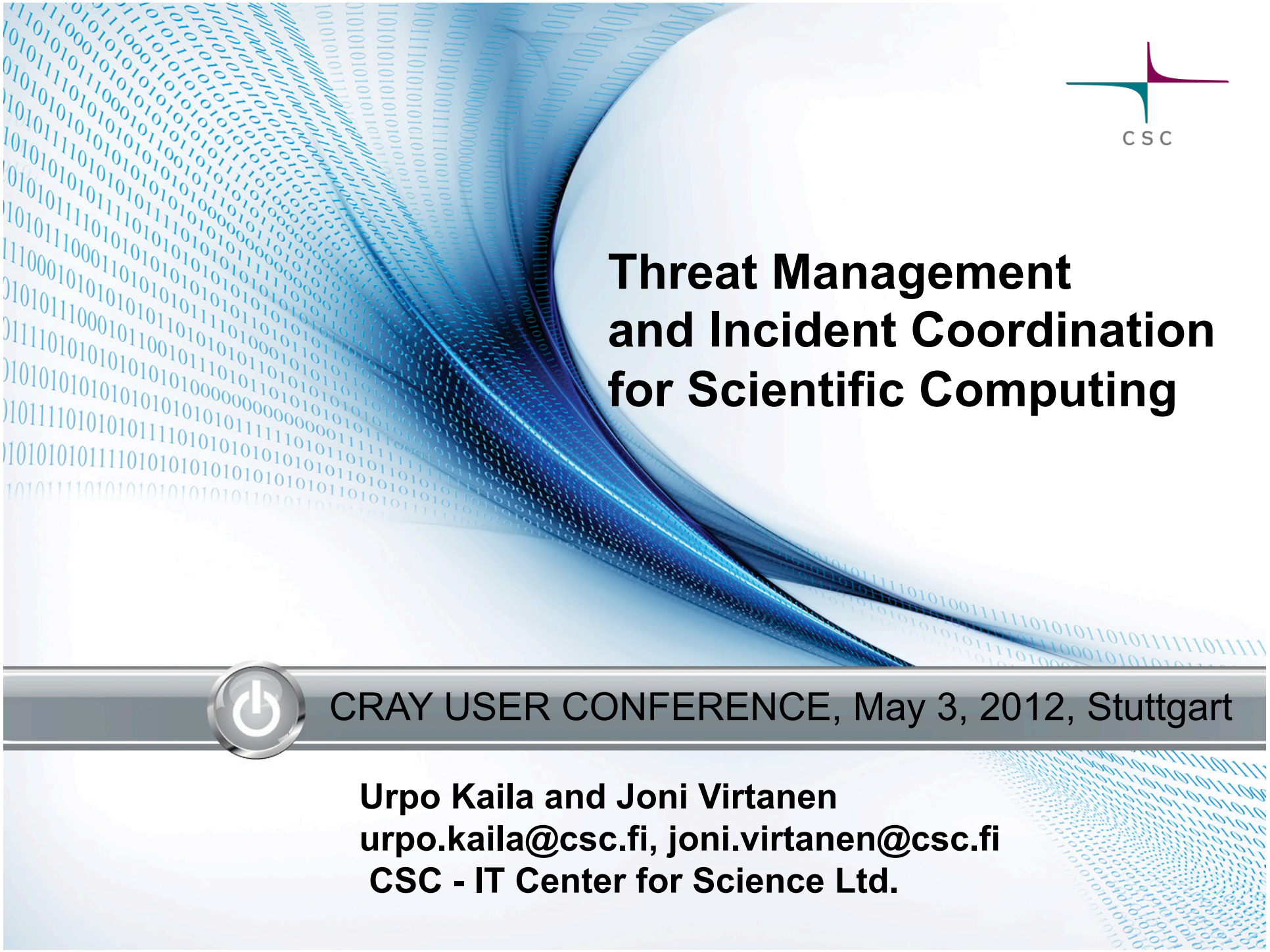
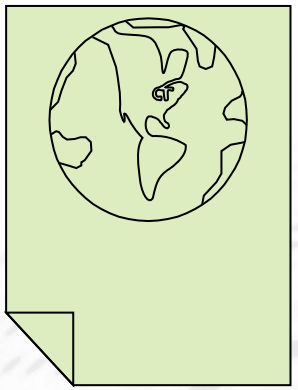


Threat Management and Incident Coordination for Scientific Computing

CRAY USER CONFERENCE, May 3, 2012, Stuttgart

Urpo Kaila and Joni Virtanen
urpo.kaila@csc.fi, joni.virtanen@csc.fi
CSC - IT Center for Science Ltd.

Outline



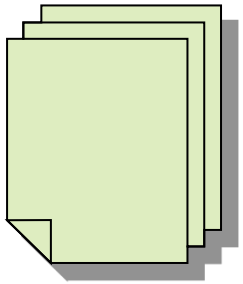
- Introduction
- On Security
- The poll
- Results
  - Background
  - Current Threat Management and Incident Handling
  - Developing Threat Management and Incident Coordination
- Discussion and Conclusions

Introduction

- Researchers wants reliable and flexible access to high performance computing - security is not always of the primary concern
- … until a security incident endangers user data and credentials or generic availability of site services
- There is growing demand for a more structured cooperation between sites for both proactive threat management and reactive incident coordination
- … but how?

Security = Confidentiality x Integrity x Availability

- Information security is not only about deploying technical security controls, it is also about dynamical decision making in a complex environment
- As in warfare situational awareness and knowing your ‘enemy’ is one of the key factors for successful defense
- Intentional incidents vs. faults or errors – a narrow or broad view on security
- NIST => security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices
- Read Bruce Schneier's new book on Trust (Liars and Outliers)



The paper

- we will show **how data centers currently identify common threats and coordinates information security incidents among sites** and other players, such as vendors, open source software providers and Computer Security Incident Response Teams (CSIRT)
- we will study how different sites and actors **would like to see information security measures developed in the in the future**

The Poll 1 (2)

- A short open poll was sent out in late April 2012 to a set of open or closed targeted email lists
- Implemented with SurveyMonkey (leading poll tool)
- Ten questions
  - Background (1-6)
  - Current Threat Management and Incident Handling (7-9)
  - Developing Threat Management and Incident Coordination (10)
  - 7. and 10. complex ranking questions

The Poll 2 (2)

- Target groups used by the authors:
  - Persons responsible for computer security and incident handling at sites running Cray hardware
  - Several email list for the PRACE*
  - Several email list for grid computing
  - TERENA** CSIRT teams
  - EUDAT*** Operations lists
  - Site Security Officers
  - Forwarded requests

* Partnership for Advanced Computing in Europe

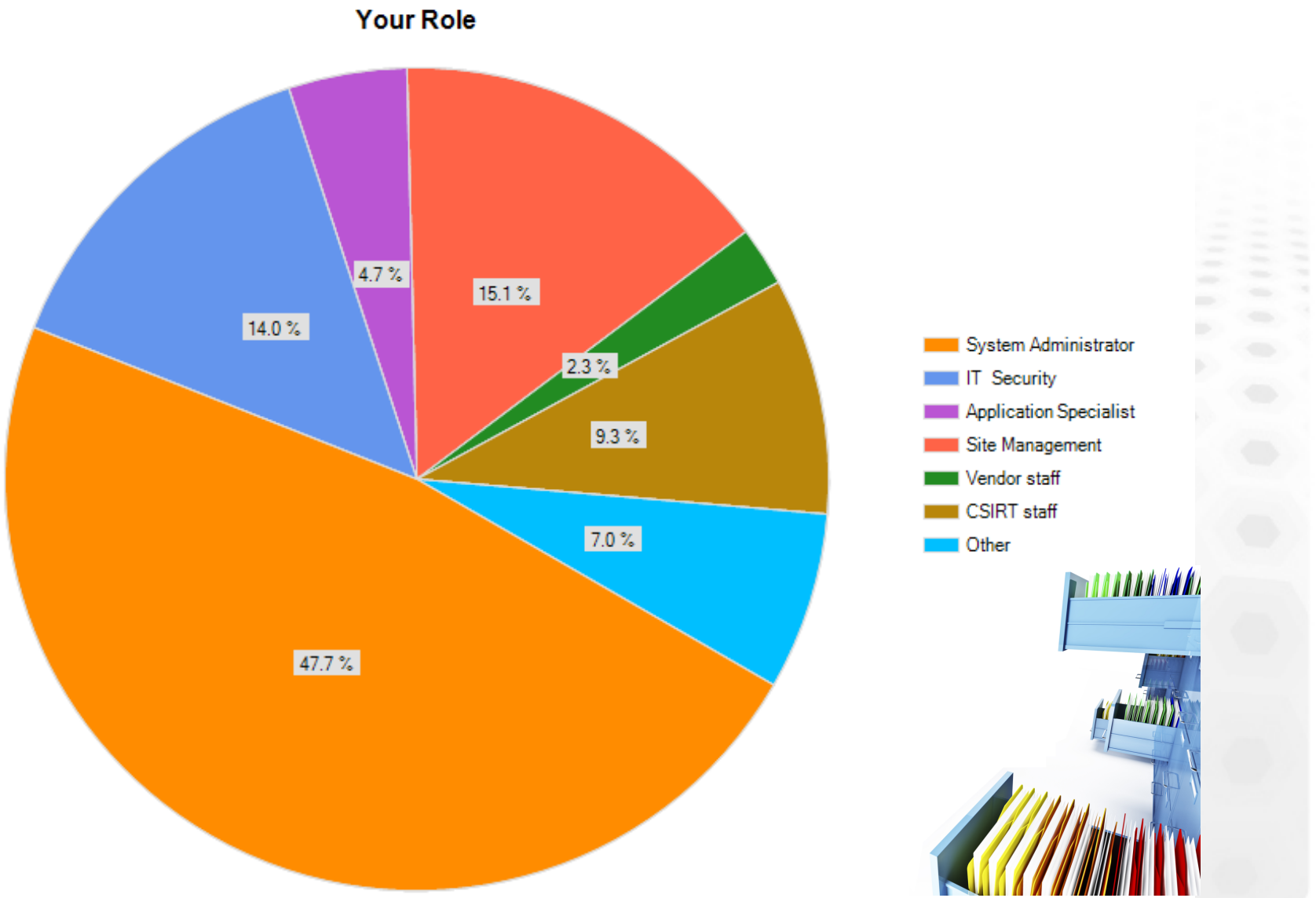
** Trans-European Research and Education Networking Association

*** A Collaborative Data Infrastructure in Europe

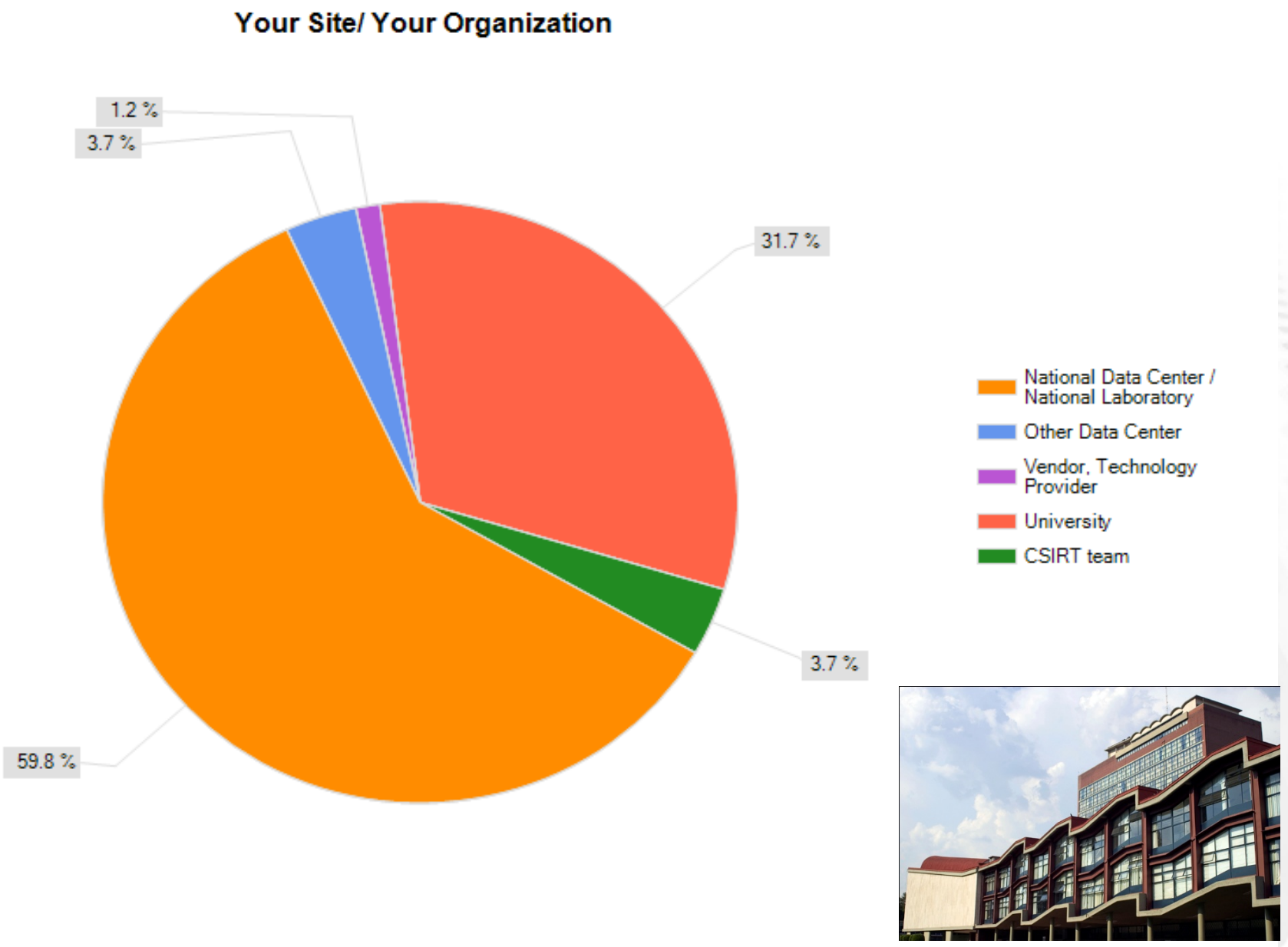
Poll Data

- 86 answers were received
  - 50 respondents answered all questions
  - 56% answered question 10.
- A bias to Europe and USA
- Several reasons for fewer answers for t
  essential security questions.
  - Too complicated or complex questions?
  - Unclear questions, errors?
  - Incoherent questions?
  - Alternatives not experienced as good enough?
  - Too tedious or too time consuming?
  - Did not know any good answers?
  - Sensitive/classified information?

Background 1 of (4)

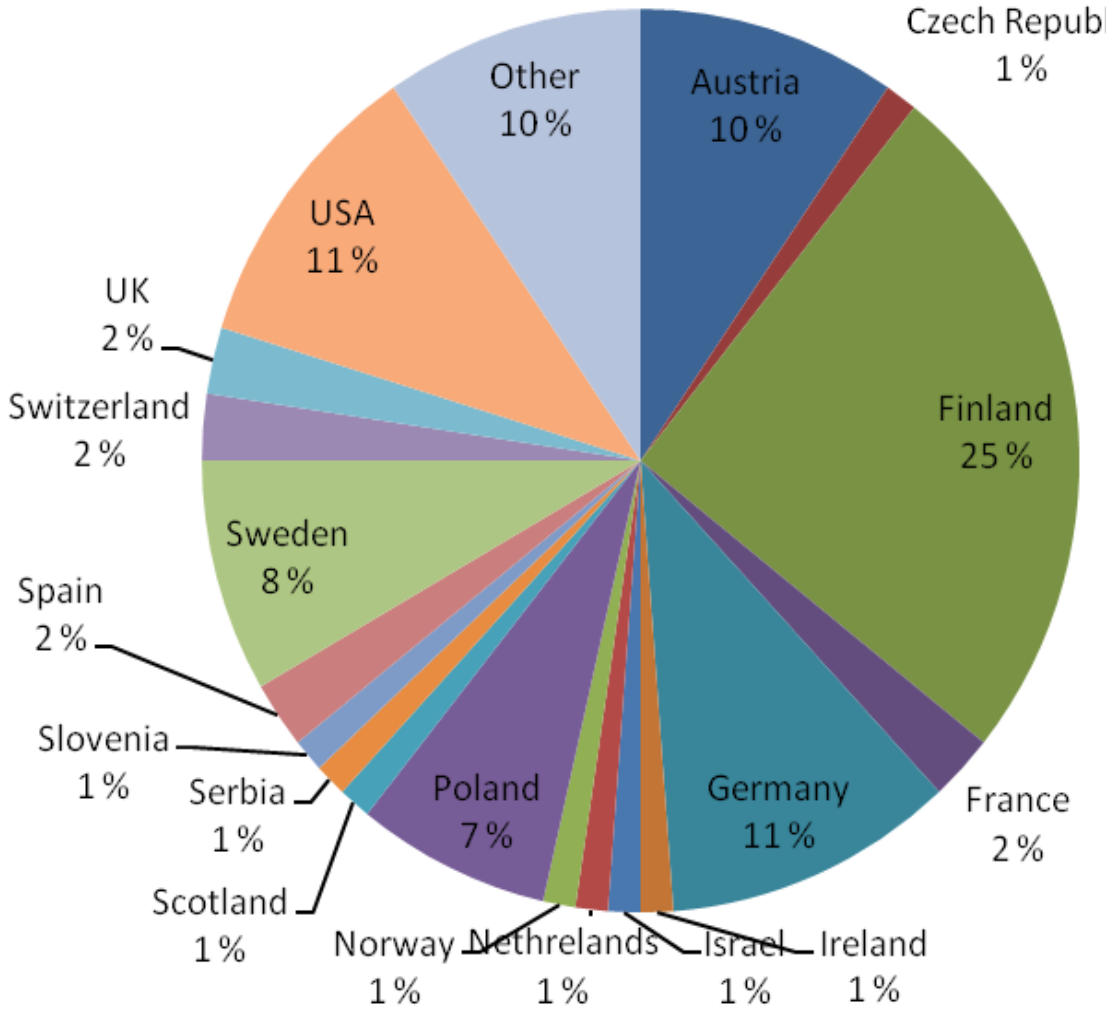


Background 2 of (4)



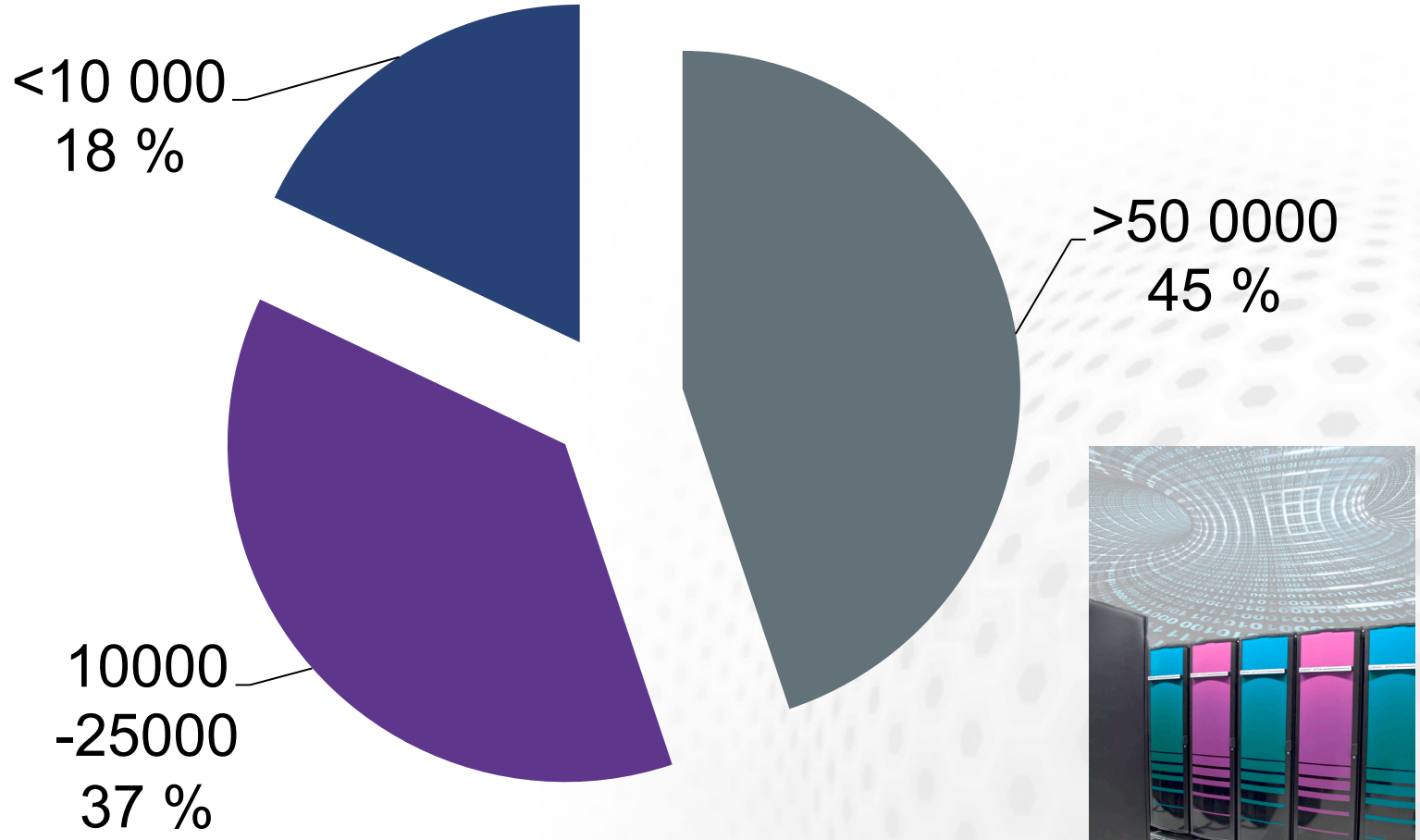
Background 3 of (4)

Country

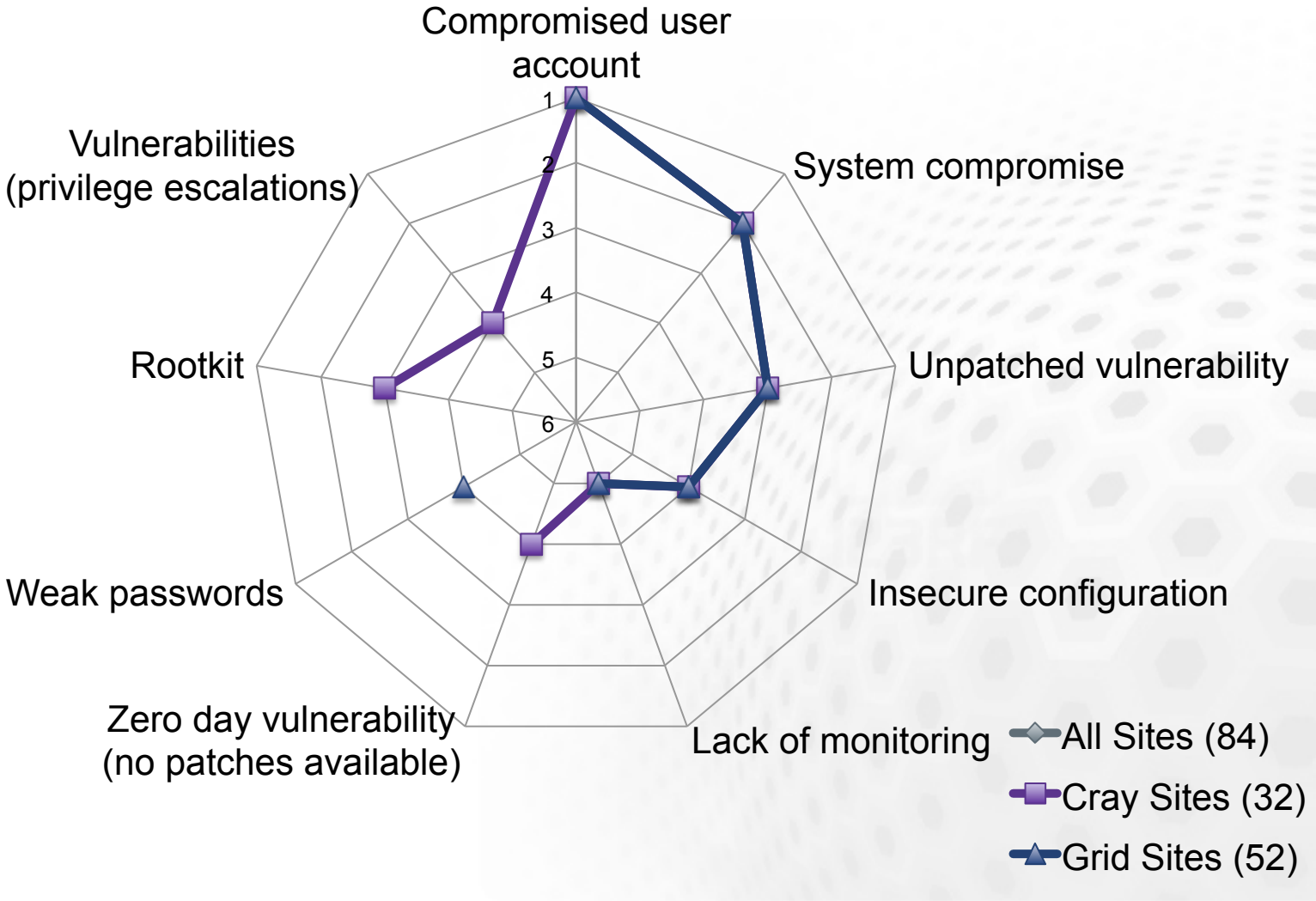


Background 4 of (4)

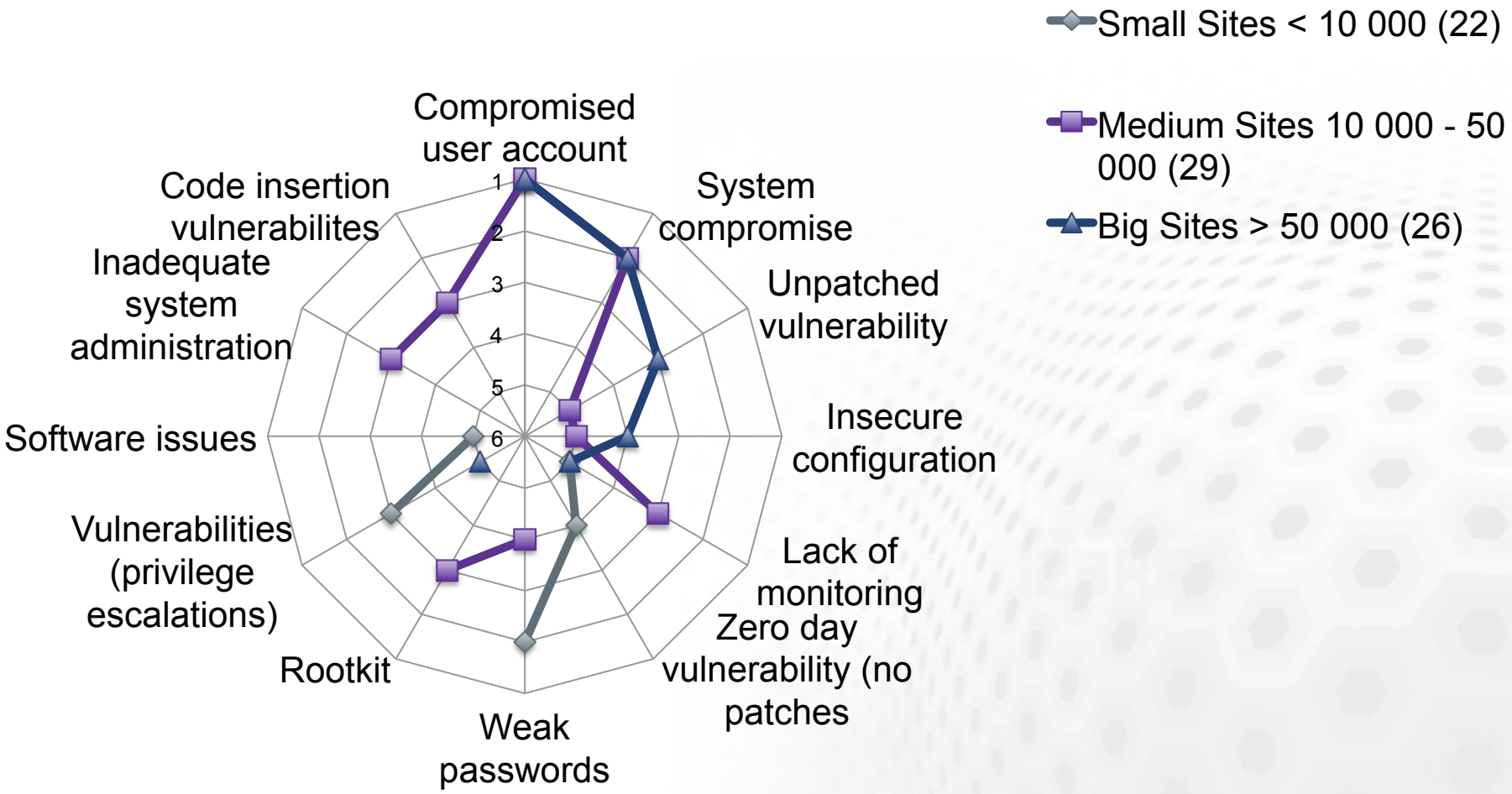
Site Capacity (# of Cores for scientific computing)



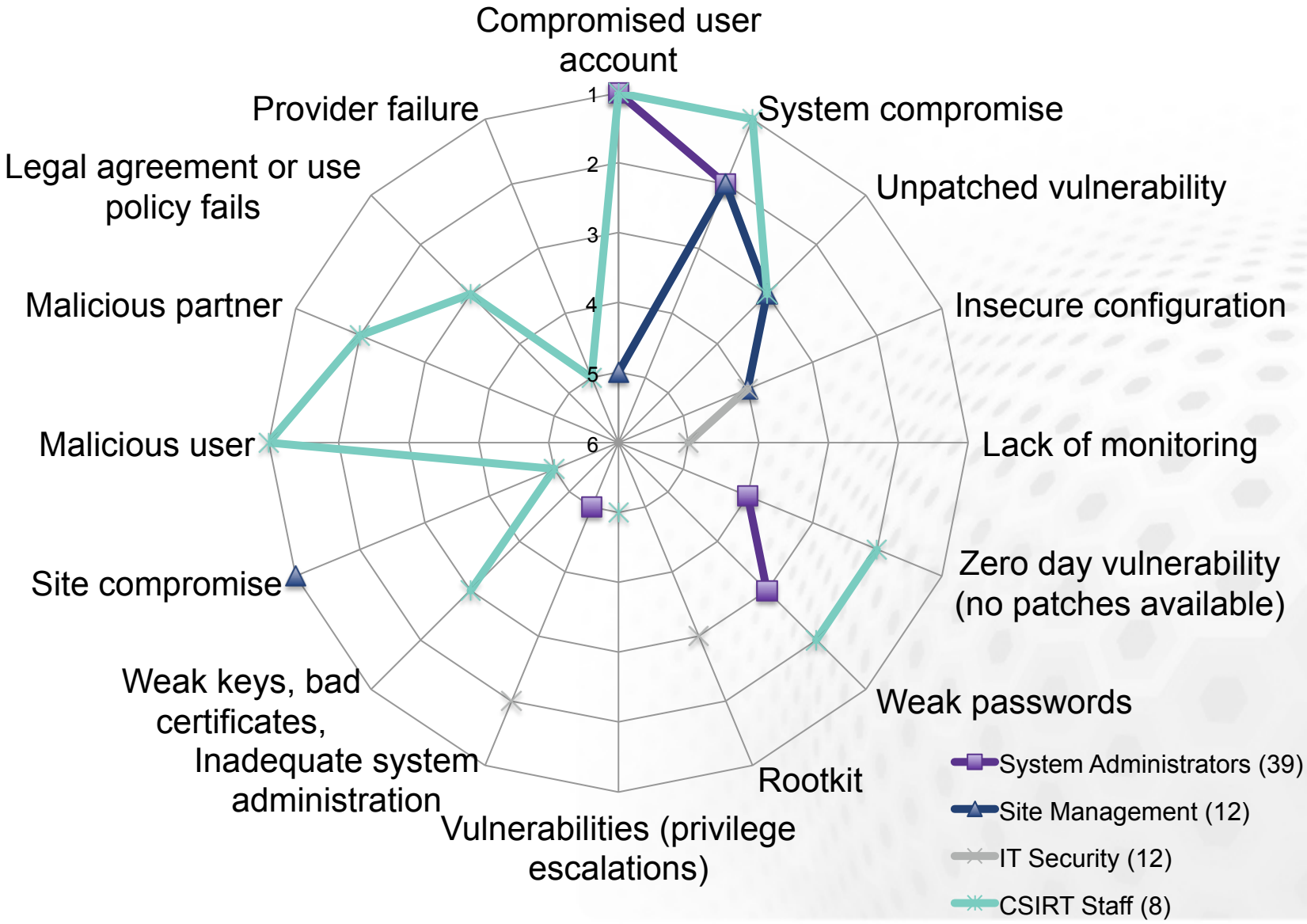
What are the FIVE worst security risks endangering computing services? All Sites / Cray Sites / Grid Sites



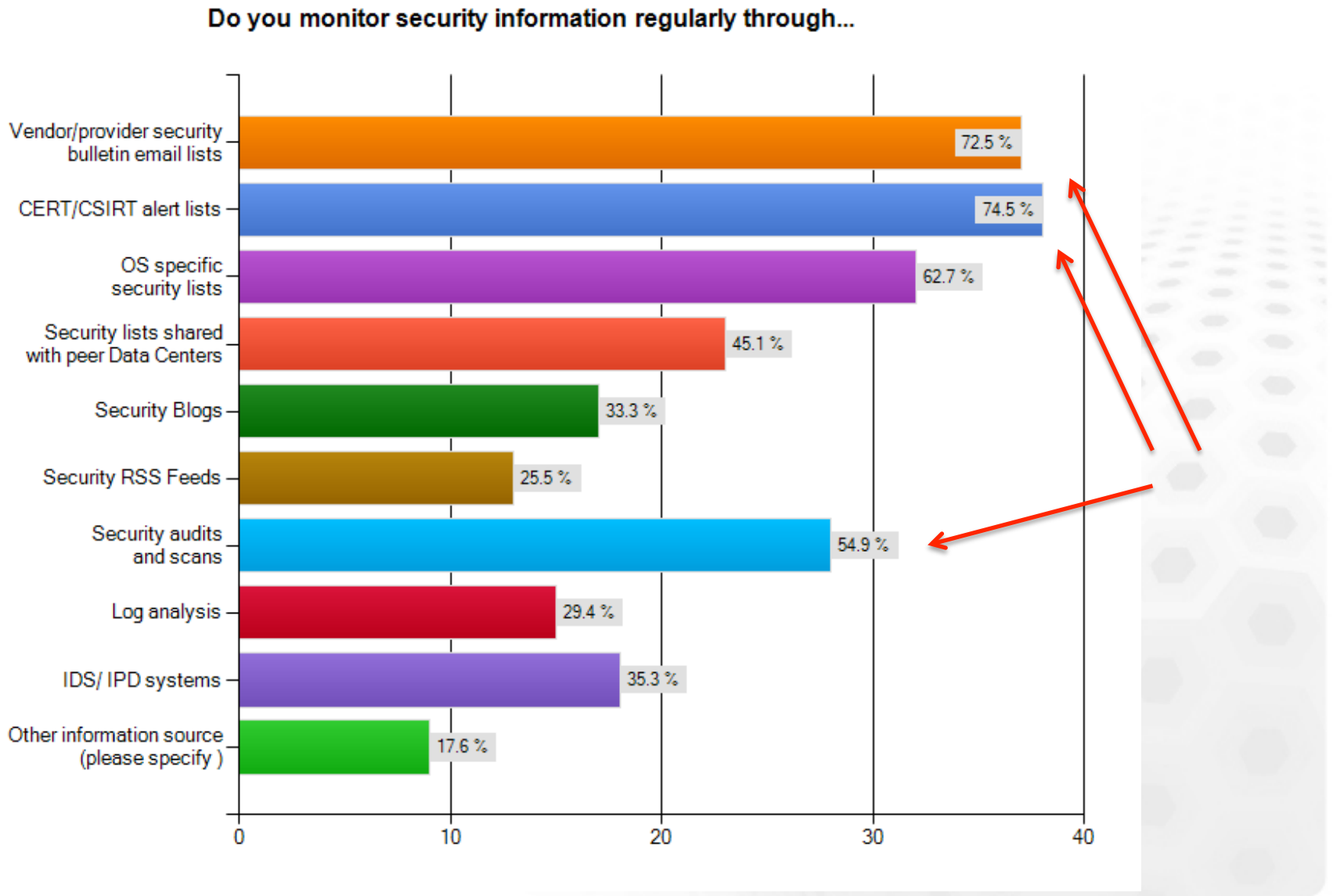
What are the FIVE worst security risks endangering computing services Per site size



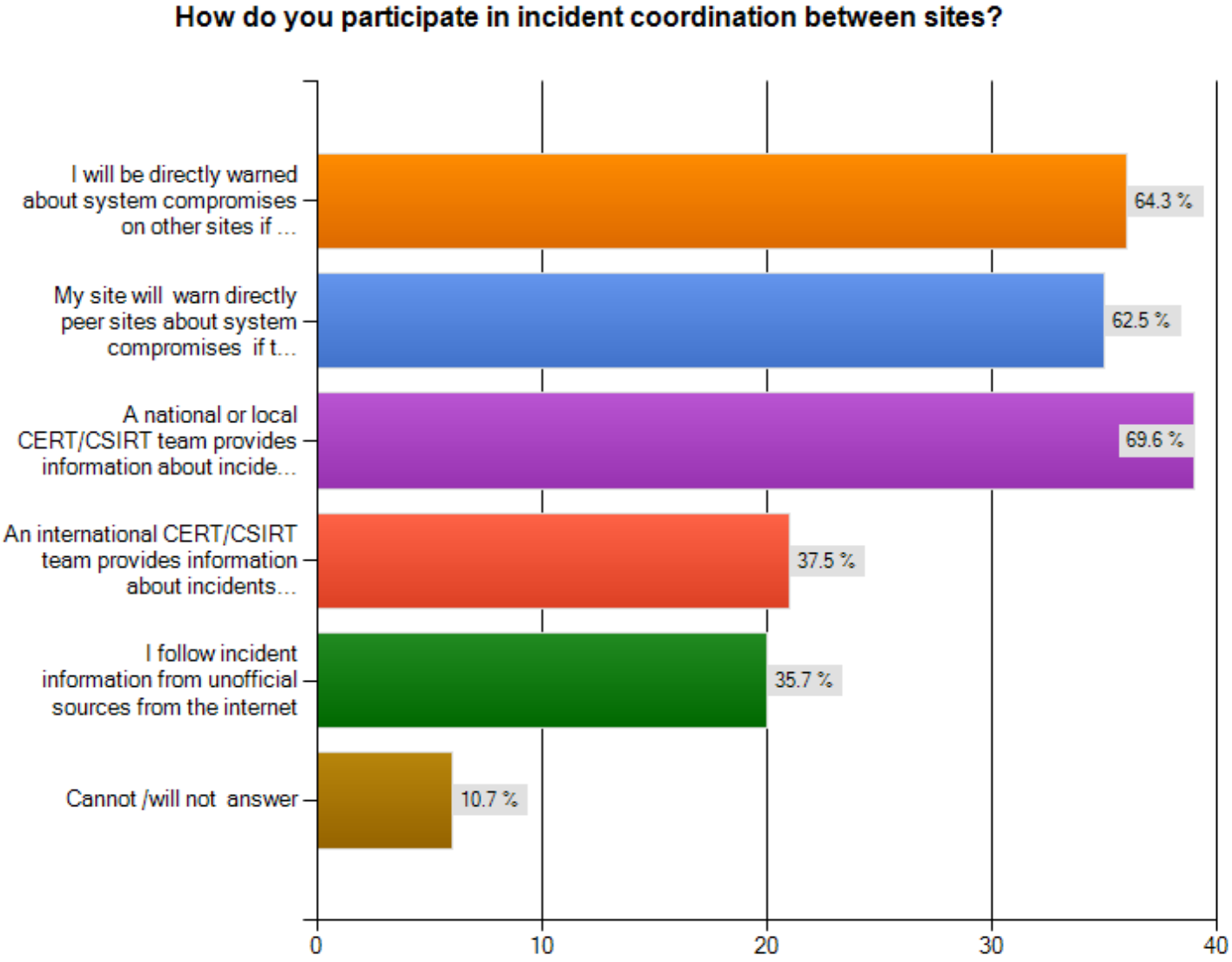
What are the FIVE worst security risks endangering computing services Per role



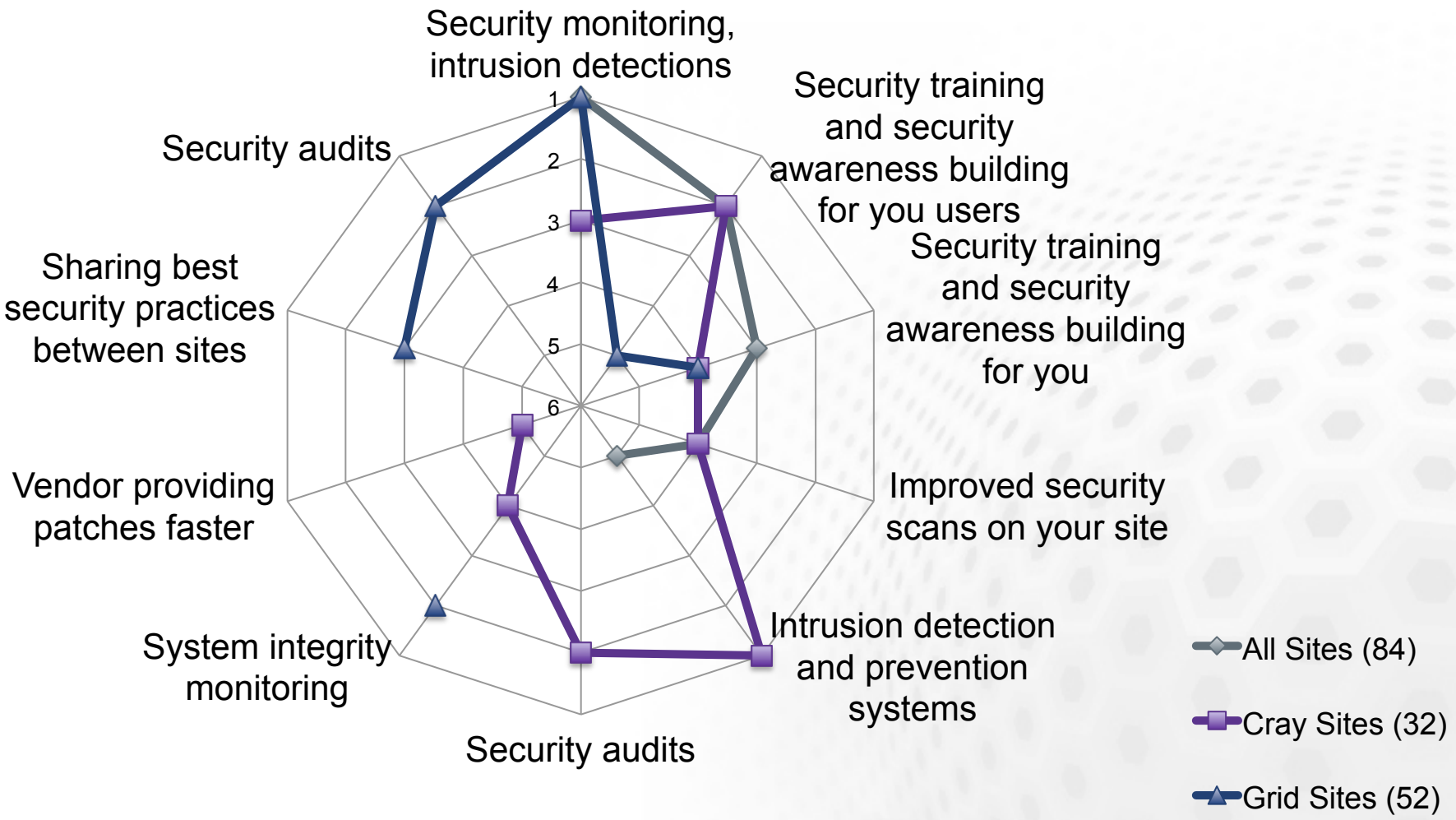
Current Threats and Incident coordination



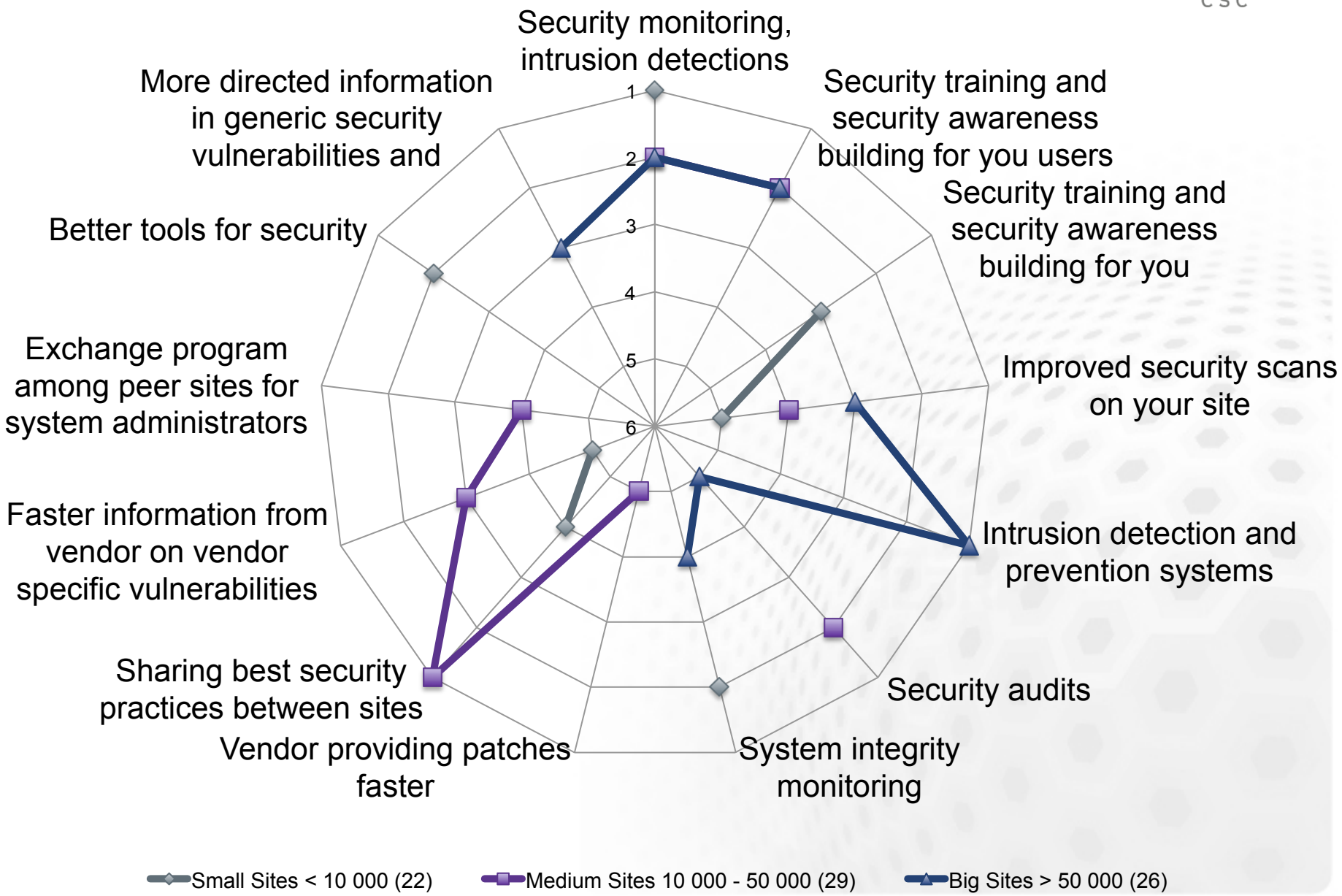
Current Threats and Incident coordination



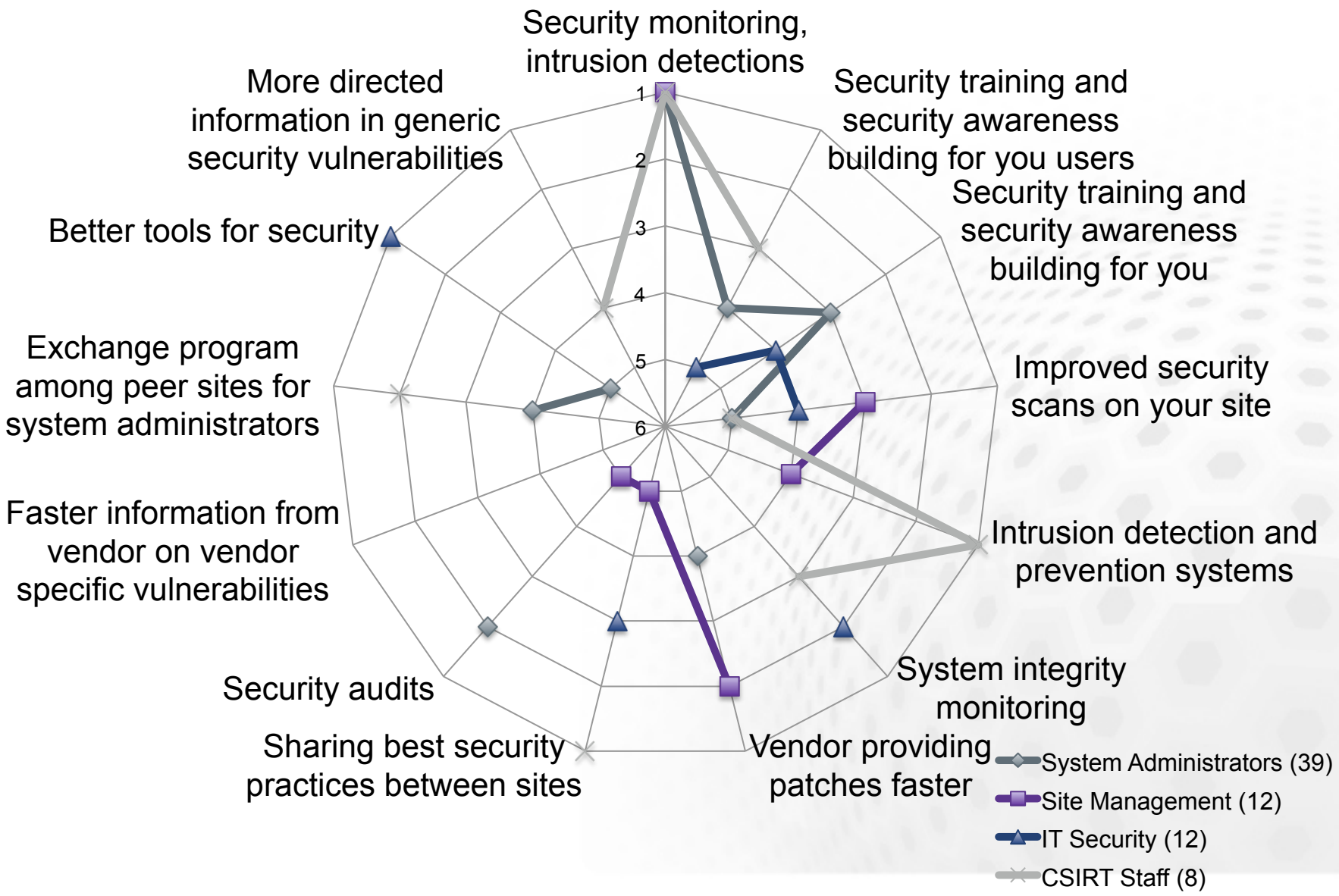
What measures would improve threat management and incident coordination on your site – Cray sites and other



What measures would improve threat management and incident coordination on your site – size of site

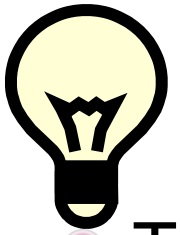


What measures would improve threat management and incident coordination on your site – per role



Results 1 (3)

- From many alternatives the well known classical threats were by all sites considered as worst risks
  1. Compromised user account
  2. System compromise
  3. Unpatched vulnerability
  4. Insecure configuration
  5. Lack of monitoring
- Little variation between answers from different roles and sites
  - Managers saw site compromise as the worst risk
  - CSIRT specialists saw malicious users and partners as the worst risks



Results 2 (3)

- The sites uses a rich set of complementing sources for security information
  1. Vendor/provider security bulletins
  2. CERT/CSIRT alert lists
  3. Security audits and scans
- Most sites are engaged in incident coordination between sites
  1. A national or local CERT/CSIRT team provides information about incidents
  2. will be directly warned about system compromises on other sites if my site is affected
  3. My site will warn directly peer sites about system compromises if the compromise might affect them

Results 3 (3)

- The measures that would mostly improve threat management and incident coordination
  1. Security monitoring, intrusion detections
  2. Security training and security awareness building for users
  3. Security training and security awareness building for administrators
  4. Improved security scans on your site
  5. Intrusion detection and prevention systems

Discussion and Conclusions

- Our sites already monitor security information pretty well - and shares the information to peers
- To yet improve security:
  - Keep up the good work with CUG Conferences!
    - We need more papers on system administration and security
  - Implement shared information security training and expert exchange programs between sites
    - Which sites would like to participate? Contact us.
    - Would Cray be interested to facilitate this?

  More joint work also needed to improve tools and practices for security monitoring, intrusion detection and security scans
  - Fast and reliable information from Cray on vulnerabilities and patching is also very important
    - CSIRT functions and liaisons also to be developed