Access denied? Managing access to the Web within the NHS in England: technology, risk, culture, policy and practice

Catherine Ebenezer
PhD student, Information School, University of Sheffield

Health Libraries Group Conference, Scarborough
16th September 2016

Supervisors:
Professor Peter Bath, Professor Stephen Pinfield

The University Of Sheffield.

"People assume that abusing the Internet is an IT problem … it isn't an IT problem, it's a management problem."
Retired NHS IT manager

Shouldn't we be managing the risks more effectively in order to allow learners the freedom to use IT resources to better effect?
Prince et al. *(2010, p. 437)*

Information School

The University Of Sheffield.

Overview

- Introduction and background
- Web application blocking: earlier findings
- Research questions and issues
- Methodology and methods
- Web use at work – a risk?
- Approaches to managing information security
- Secure web gateways / web proxies
- False positives – the ROC curve
- Findings / Discussion
- Recommendations
- Questions

Information School

Introduction and background

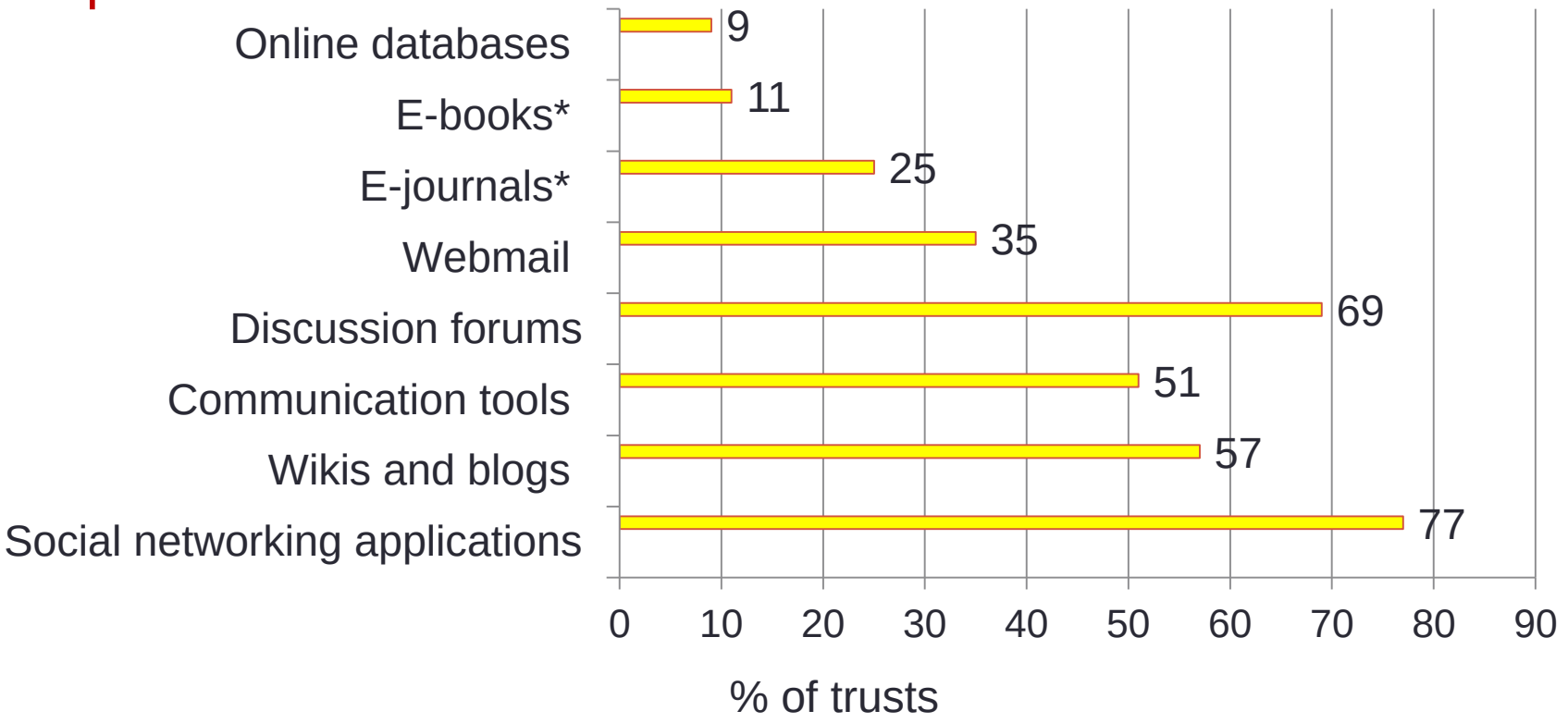
- LIS Manager in mental health NHS FT 2008-2012
- Variety of technological barriers / hindrances to information seeking, teaching and learning, clinical and management decision-making
  – ascribed variously to:
  - Information governance/ information security
  - IT infrastructure policies and practices
  - Communications policy
- Blocking of ‘legitimate’ websites
- Obstacles to use of particular content types and applications
- Social media / Web 2.0 a particular problem
- *Implications?*

The University Of Sheffield.

Information School

Web application blocking

Impacts



SHALL IT subgroup survey of NHS librarians (2008)

The University Of Sheffield.

Research questions / issues

- The nature and extent of restrictions on access to the World Wide Web within NHS organisations arising from organisational policies and practices
- Their impacts on professional information seeking and sharing, and working practices in general
- The attitudes, presuppositions and practices which bear on how web filtering is implemented within NHS trusts, in relation to overall organisational strategies

---

- Web filtering devices and their limitations
  Differing stakeholder perspectives involved
- Attitudes to / assumptions about (information governance, information security) risks
- *NB distinction between websites and web applications*

Information School

Part of a wider study of access to information for learning and teaching

Methodology and methods

Exploratory case study

- Unit(s) of analysis
  - One or more NHS trusts of different types (DGH + community services, MH + community services, teaching hospital)
- Methods
  - Semi-structured interviews with key informants (10+ per trust)
    - selected via purposive / snowball sampling
    - representing a variety of perspectives:
      - Clinician education and staff development
      - Library and information
      - Communications
      - Information governance
      - IT management, esp. network security and PC support
      - Human resources
      - Workforce development

Methodology and methods

Exploratory case study

- Methods (cont'd)
  - Interviews with other key informants: NHS Evidence, medical school e-learning lead, secure web gateway vendor
    - Gained additional perspectives
  - Documentary analysis – selective / *ad hoc*
    - Background
    - Policies and strategies: IT, LIS, workforce development, information governance, Internet AUPs
    - Codes and standards
    - Reports and reviews
    - Statements of values
    - Security device documentation
  - Thematic analysis using NVivo

The University Of Sheffield.

Information School

The University Of Sheffield.

Web use at work – a risk?

Categories of potential risk to the organisation:

- Legal – *employers can be legally liable for staff accessing and distributing illegal material*
  - Child pornography and other obscene material or racially inflammatory material, racial or sexual harassment, discrimination, hacking, the defamation of management, customers or competitors, software piracy, copyright infringement, fraud, and breaches of the Data Protection Act
- Security - *???* *risks from websites and web applications*
  - Web-borne malware – major security threat – *but ….*
  - NB *not* a close correlation between subject matter of web content type of content and malware risk - *Provos* et al. *(2008)*
- Productivity - *???*
  - Network bandwidth clogged / performance degraded
  - Staff wasting time
  - Positive effects?

Information School

The University Of Sheffield.

Approaches to managing information security (adapted from Fléchais *et al.*, 2006)

	Category	Description	Example
Technical	Prevent	Stop attacks from occurring	Firewalls, secure web gateways, access control etc.
	Detect	Notice and identify attacks	Monitoring of web use – *not routinely permitted under UK law*
	React	Stop or mitigate an attack	Automated response systems linked to intrusion detection systems
	Deter	Discourage misuse	Visibility of countermeasures
Social	Prevent	Stop attacks from occurring	AUPs; rules on locking screens, rules against p/w sharing, etc.
	Detect	Notice and identify attacks	Sysadmins, alert users, auditing
	React	Stop or mitigate an attack	Sysadmins or emergency response teams
	Deter	Discourage misuse	Prosecution, disciplinary action

The University Of Sheffield.

Secure web gateways / web proxies

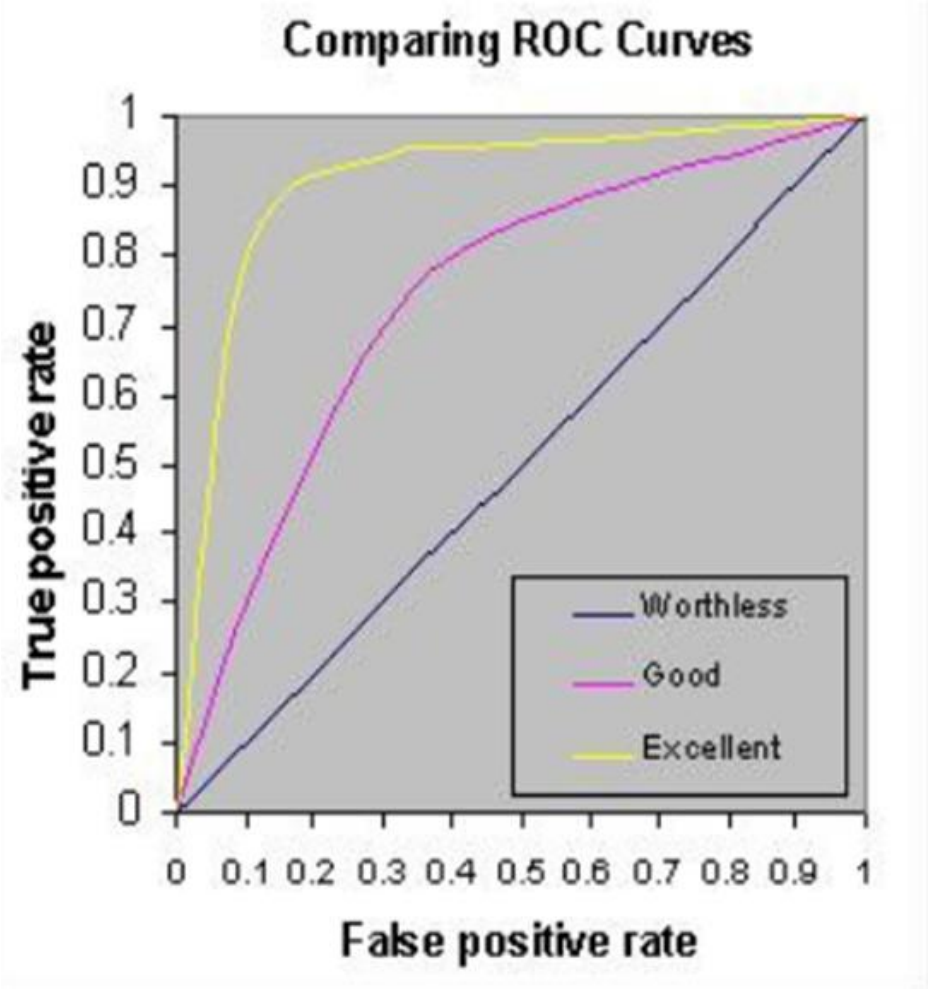
- Sit at perimeter of organisation's network – enforce acceptable use policies
  - Commonly in use: Forcepoint (formerly Websense), Smoothwall, Bloxx, Trustwave WebMarshal, Webroot, etc.
- Two roles:
  - Authorisation and authentication / filters 'inappropriate' content
  - Blocks web-borne malware
    - SWGs are able to categorise URLs and to analyse and manipulate scripts on web pages
- Main mechanisms:
  - Blacklists (may be third-party)
  - 'On the fly' via machine learning / content categorisation
    - 'black box' – commercially confidential

Information School

The University Of Sheffield.

False positives / the ROC curve

As sensitivity increases, specificity / accuracy declines



Zhang and Janssen, s.d.

Information School

The University Of Sheffield.

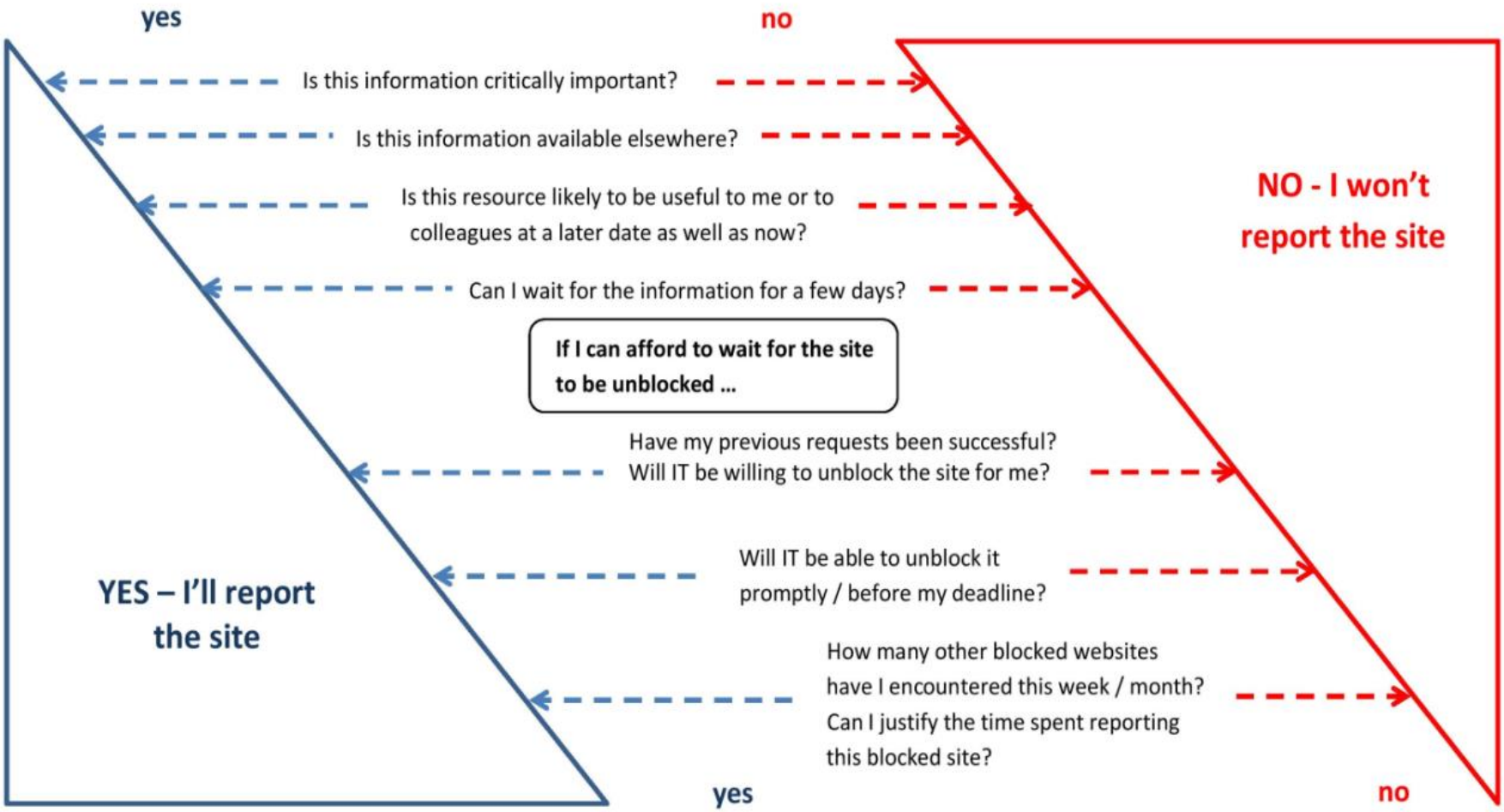
Results

- Blocking of websites a problem frequently reported to NICE by librarians
- **District general hospital (DGH)** and **mental health services (MH)** reported very few instances of website blocking
  - When a legitimate website blocked, IT department had unblocked it promptly once reported
  - Pharmacists most affected; instances of website blocking at MH usually related to substance misuse, eating disorders or sexuality
- Staff at **teaching hospital (TH)** experienced greatest number of obstacles to information-seeking caused by blocking of legitimate websites
  - Reported frequencies of blocking varied from ‘every two months’ to ‘constant’ or ‘daily, probably’
  - Affected the work of clinical educators in particular
- Most blocked sites not reported to IT department

Information School

The University Of Sheffield.

Results



The University Of Sheffield.

Results

- Much decision-making in relation to information security issues was tacit – IT managers did not explicitly discuss risk
- ***IT security managers reported not having time to evaluate the effectiveness or impact of the SWGs they deployed***
  - Depended on reports from users (via calls logged with trust helpdesk) of false positives
- ***Likely to accept default configurations and categorisations of content offered by suppliers***
  - IT manager at TH appeared aware (via emails sent to him) of the inconvenience caused to users by false positives
- Main focus of attention and concern at TH and MH: ***potential security risks or impact on network traffic presented by 'recreational'/ non-work use*** of the web

Information School

The University Of Sheffield.

Results

- TH had explicit policy of blocking advertising
  - Claimed to mitigate potential security threat of ‘malvertising’ (web-borne malware spread via syndicated advertising)
  - Sometimes seemed to have effect of blocking entire site content
  - Likely factor in high number of blocked websites
- Possible factor: TH SWG’s lack of specificity in identifying and blocking inappropriate or compromised content
- ***Neither librarians nor IT managers aware of national whitelist of sites not to be blocked***
- No relationship found between IG / IT structures and levels of blocking
  - But communication between IT and IG in TH very poor

Information School

The University Of Sheffield.

Discussion

- "First, do no harm …"

  Hippocratic oath

- IT staff should be at pains to avoid blocking the good when attempting to prevent the bad *(Verma* et al., *2012)*

- "Users … don't pursue innovative ideas because they can't face any more 'battles with security' that they anticipate on the way to realising those ideas"
- Users' experiencing false positives reduces the overall credibility of information security
- *(Sasse, 2015)*

Information School

The University Of Sheffield.

Recommendations

- National whitelist:
  - Efforts needed to engage librarians with reporting / maintenance / updating
  - Put in place robust local systems for IT departments to be notified of updates
- Responses to information security incidents should be proportionate
- IT and IG departments should:
  - encourage the reporting of false positives as applicable
  - institute processes for responding promptly to unblocking requests
  - consult more widely with stakeholders in the development and revision of Internet AUPs
  - publicise / consult on web filtering practices and monitor and evaluate their impacts – part of policy process
  - establish enhanced levels of access to web content for clinical and clinical support staff groups (e.g. librarians)

Information School

The University Of Sheffield.

Questions?

Catherine Ebenezer
lip12cme@sheffield.ac.uk
http://www.mendeley.com/profiles/catherine-ebenezer1/
@ebenezer1954

Information School

References

- Blenkinsopp, J. (2008). Bookmarks: web blocking – giving Big Brother a run for his money. *He@lth Information on the Internet,* (62), 2008.
- Fléchais, I., Riegelsberger, J., & Sasse, M. A. (2006). Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In Proceedings of the 2005 workshop on new security paradigms (pp. 33–41). ACM.
- Prince, N. J., Cass, H. D., & Klaber, R. E. (2010). Accessing e-learning and e-resources. *Medical Education*, 44 436-437.
- Provos, N., Mavrommatis, P., Rajab, M. A., & Monrose, F. (2008). All your iFRAMEs point to us. Mountain View, CA. http://research.google.com/archive/provos-2008a.pdf
- Renaud, K., & Goucher, W. (2012). Health service employees and information security policies : an uneasy partnership? *Information Management and Computer Security*, 20(4), 296–311.
- Sasse, M. A. (2015). Scaring and bullying people into security won't work. *IEEE Security and Privacy*, (June), 80–83.
- Technical Design Authority Group (2008). TDAG survey of access to electronic resources in healthcare libraries. London: TDAG.
- Verma, S., Kavita, & Budhiraja, S. (2012). Internet security. *International Journal of Computer Applications in Engineering Sciences*, *II*(III), 210–213.
- Zhang, W., & Janssen, F. (s.d.). The relationship between PR and ROC curves. Darmstadt: Technische Universität Darmstadt. http://bit.ly/2cpN7LO