

Craig L. Roth KnowledgeForward, 2543 N. Greenview Avenue, Chicago, IL 60614
www.knowledgeforward.com craig.roth@knowledgeforward.com 773.868.0266

October 2005

BROWSER WARS II: WHAT OWNERS OF CUSTOMER-FACING WEBSITES SHOULD KNOW

By Craig Roth

Alternatives to Microsoft's ubiquitous Internet Explorer browser are starting to make headway in the consumer market. As usage of minority browsers such as Firefox and Opera slowly increase, increasing browser compatibility of customer-facing websites and improving handling of incompatibility when it occurs will become more important. Extrapolating market-wide browser usage and consumer security concerns into guidance for web development is necessary to ensure that an organization's customer-facing websites will not be rendered unusable by users with old browsers or killed by popup blockers.

Most companies are targeting the most common combinations and understand that some small percentage (1%-5%, depending on the audience) may have difficulty using their site, ranging from pages that render unattractively to total inability to access content or features. Figure 1 shows the percentage of organizations

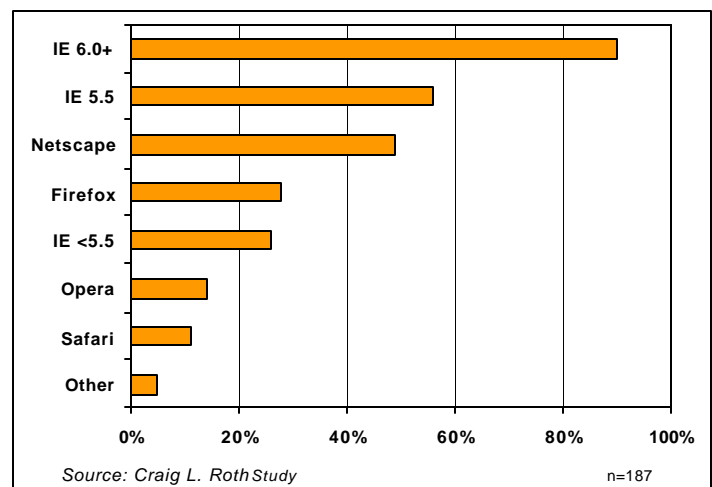


Figure 1 - % of Large Sites Testing Against Browser

that test against various browsers, and demonstrates that testing the latest two versions of IE and Netscape is generally considered sufficient, although we recommend testing against Firefox instead of Netscape. Even though they are both based on the Mozilla engine we believe Firefox has more momentum. From a review of publicly available statistics, around 65% of all browsers are IE6, 15% IE5.5, and 12% IE5.0. A number of sources exist to provide up-to-date browser statistics (e.g., WebSide Story is the most prevalent), however every website has a unique mix of users that skews the statistics. For example, having more users from the education, government, and engineering sectors will increase the number of minority browsers due to their prevalence of Unix desktops and open source software. Ultimately, the most relevant statistics are the ones that come from an organization's own web sites, so building metrics into websites is critical for making minority browser support decisions and tracking trends. This is the only way to accurately determine an organization's specific browser mix.

It is unrealistic to expect that a website can be created to support 100% of customers' browsers unless pure HTML 3.2 is sufficient. Therefore, business and IT should jointly analyze customer patterns, browser metrics from the web logs, customer value metrics, and channel switching costs to negotiate an acceptable service level that IT can commit to support with development and testing and that the business can tolerate.

Unsupported users should be gracefully switched to another channel (i.e., email, live chat, call center, storefront). Customers are currently doing their own channel switching when encountering browser issues rather than calling the technical helpdesk, as only 7% of the helpdesk calls relate to browser-specific problems. A recent survey of ours found that 65% of organizations have no specific service level, and this figure is even higher in some industries (71% of government agencies, 80% of educational institutions). Of those that have a service level, <99% is most common (47%) followed by 99.99+% (25%).

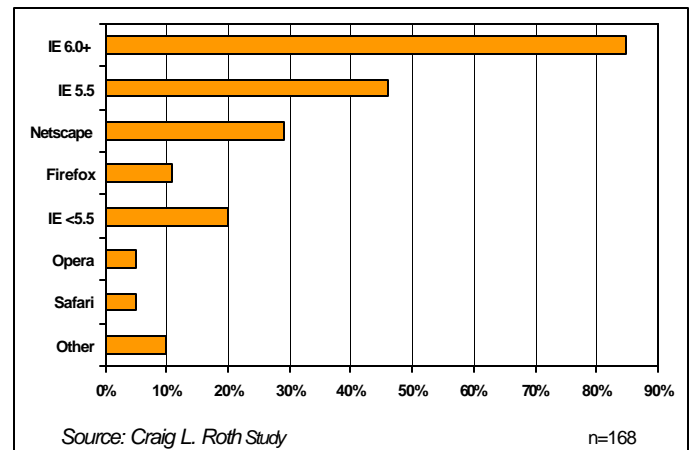


Figure 2 - % of Sites with Helpdesk Scripts by Browser

To increase the service level, a shadow site can be developed - a "click here for text-only Web site" option that points to a lowest-common-denominator HTML version of the site. Organizations should do a cost/benefit analysis to determine if the cost of developing a shadow site exceeds that of disenfranchising the unsupported users.

WHAT SITE DEVELOPERS, TESTERS, AND SUPPORT PEOPLE SHOULD DO

Organizations should ensure that standards documents address browser issues that are relevant to web developers, testers, and support:

Guidance for web developers should address:

- Use of cookies - At this time cookies are the most common practice for maintaining state, but they have proven problematic as users become more mobile (i.e., expecting to access their information from an internet café while traveling), more consumers learn to increase security settings that reject cookies, and organizations enact stricter security policies. However, alternatives to cookies are also problematic (server-side cookies where session IDs are passed as parameters prevent bookmarking, hidden variables in pages only last for a single session), so cookies are a necessary evil and should only be used when required. If cookie information is sensitive it should be encrypted to protect the user from packet sniffers
- Use of popups – Popups should be avoided. We predict the number of consumers blocking popups (often without even knowing they are doing so) will exceed 75% by 2008, which will stress technical support and alternate transactional channels
- Minority browser policy – A policy should specify thresholds (good: “we will support any browser version used by more than 1.75% of our users, with no more than 8% of all users being unsupported, and will publish updated browser statistics quarterly”) rather than specific browsers (bad: “We will support IE 6.0 and Firefox”) to ensure it is consistently relevant. It should also contain the maximum number of users that will be unsupported. Support of a browser implies regression testing against that specific browser version as well as helpdesk scripts.
- When to use shadow sites – Shadow sites are stripped down duplicates of rich internet sites. A “click here for HTML site” option can be a lower cost way to address the testing, support, and channel switching issues that come

Behind the Analysis

A view into the historical and market precedents that guide this analysis:

Lies, Damn Lies, and Statistics: Statistics for IT-related studies are often skewed by the survey population. Surveys that concern counter-Microsoft technologies are often skewed by over-representing non-corporate users

It's easier to code than support: Many fancy things can be done with new technology, but user support (their hardware/software capabilities and helpdesk requirements) can spoil the fun

with using richer internet technologies. Currently, shadow sites are used mostly by sites that make extensive use of Flash, but this concept is expected to trickle down to less extravagant sites over the next few years. Explore usage of a network-based device that can segment traffic to shadow sites automatically based on the type of client technology that is available.

Guidance for the web testing team should address:

- Combinations of user settings to be tested – Guidance should address the browsers (types and versions), devices (i.e., PDA, cell phone), bandwidth, resolutions, color bit depths, and security settings (i.e., very open versus very restrictive) to be tested
- Testing tools to use – Organizations should invest in technology to help validate against different browsers. For example, Macromedia Dreamweaver allows targeting certain browsers and will indicate unsupported tags. Validation products (i.e., Coast WebMaster, Ixsite Web Analyzer) can be run against Web sites to warn about HTML tags that may not work in some browsers.

Guidance for the Customer technical support team should address:

- Acceptable time spent by an agent troubleshooting minority browser problems before recommending a majority browser – A common practice is to provide all-or-nothing support, so no browser switching recommendations would occur once troubleshooting begins
- The degree to which help documents and call center scripts will be available and continually updated for minority browsers – this policy should address which browsers will be supported for customers
- Degree of invasiveness of tech support advice to overall browser settings – Some help scripts give directions such as “accept all cookies”, changing default IP settings, or lowering security level to fix the customer’s problem. We consider this to be an ethical, corporate image, and possibly liability issue and encourage all organizations to purge their help desk scripts of steps that fix access to the organization’s website at the expense of weakening the user’s overall security or breaking other sites
- The point at which a channel switch should be recommended – Agents need to know when they can use a channel switch (away from web and toward phone, mail, or bricks and mortar store) as a last resort if they can’t solve the user’s browser problem


Note: For all the customer help desk issues, best practices for these areas have not yet emerged as few organizations have formally addressed them. The general rule is that organizations with a lower number of high lifetime customer value (LCV)

customers are more likely to ensure the highest degree of customer support, which means dedicating more time and resources to minority browser issues, being gentle with overall browser settings, and treating channel switching as a last resort. Organizations with high numbers of low (or even zero or negative) LCV customers are more likely to weigh decreased browser-incurred costs (by supporting fewer minority browsers and encouraging channel switching as a solution to browser compatibility problems) as more important than customer satisfaction. In the absence of best practices, our recommendation is to publish guidance that at least ensures consistency in customer interactions.

SUMMARY: Decisions on which browsers should be supported on a customer-facing website should be based on joint agreement between marketing and IT. Browser service levels and policies should be explicit and disseminated to web developers, testers, and technical support staff.

ENTERPRISE TAKEAWAY: Browsers are once again introducing complex issues for organizations. Issues such as the use of cookies, service levels, and browsers to be targeted need to be formally addressed for the developers, help desk, and customers.

VENDOR TAKEAWAY: Creative Agencies designing websites need to understand the technical makeup of the end users and make additional support costs clear before using rich internet technologies. Providers of rich internet technologies need to demonstrate the user of their technologies in minority browsers.

The logo for KnowledgeForward, featuring the word "Knowledge" in a yellow sans-serif font and "Forward" in a white sans-serif font, both set against a dark, blurred background of city buildings.

How KnowledgeForward can help with the issues addressed in this Opinion:

- **Cost/Benefit Analysis for Web Technology Support:** Deciding which users will not be able to get support or use certain features is a difficult decision, but 100% compatibility with advanced technology is impossible. We can provide an independent voice for determining the benefits of the technologies and the cost in terms of unsupported users
- **Web Development Guideline Design/Revision:** Organizations should have guidelines given to inhouse and external web developers that indicate policies such as acceptable technologies, browser support. We can help create these guidelines or revise them based on the need for constituency-sensitive browser support

Craig L. Roth KnowledgeForward provides assistance in planning and executing knowledge management and collaboration strategies and marketing programs. Mr. Roth is an alumnus of the META Group, where he covered enterprise portals, web site development and rich internet applications.

To learn more, please contact Mr. Roth at:

Craig Roth
2543 N. Greenview
Chicago, IL 60614

Phone: 773.868.0266

E-mail: craig.roth@knowledgeforward.com