MarketVibe

November 2008

Sorting Out the Myths When Purchasing SSL Certificates

Research conducted by:

COMPUTERWORLD

Sponsored by:

Entrust®

Contents

Sorting Out the Myths When Purchasing SSL Certificates

Overview

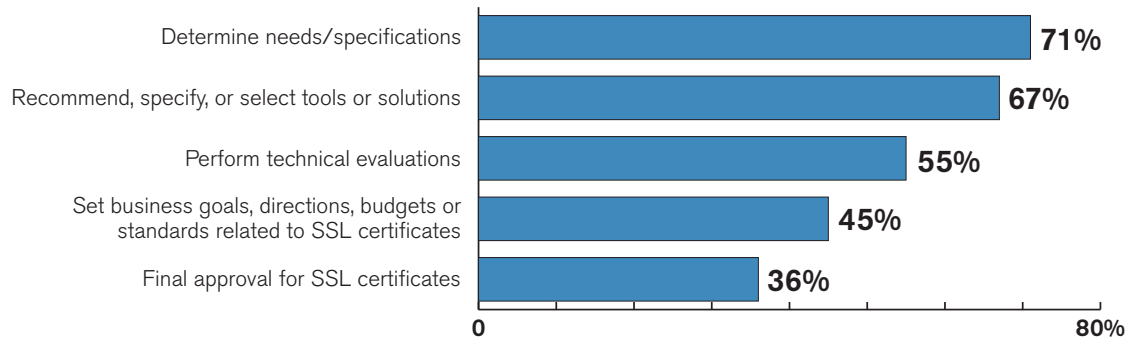
In October 2008, *Computerworld* invited IT and business leaders to participate in a survey on SSL certificates. The survey was fielded via targeted broadcasts to *Computerworld* customers, as well as through an invitation on *Computerworld.com*. The goal of the survey was to better understand current SSL certificate deployment and initiatives as well as purchase plans and vendor measures for SSL certificates. The survey was commissioned by Entrust, but the data was gathered and tabulated independently by Computerworld Research. The following report represents top-line results of that survey.

Profile of respondents

Total respondents: 103

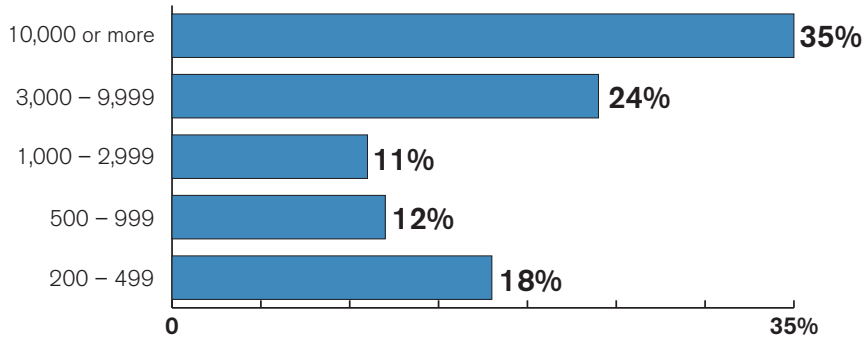
All respondents were qualified through a series of screening questions as having involvement in the acquisition of SSL certificates. All respondents are from North American locations and are employed in companies with at least 200 total employees. The chart below provides a breakdown of the percentage of respondents based on involvement in the acquisition of SSL certificates. This chart is followed by breakdowns of respondents based on company size, location, job title and industry.

How are you involved with the acquisition of SSL certificates for your organization?



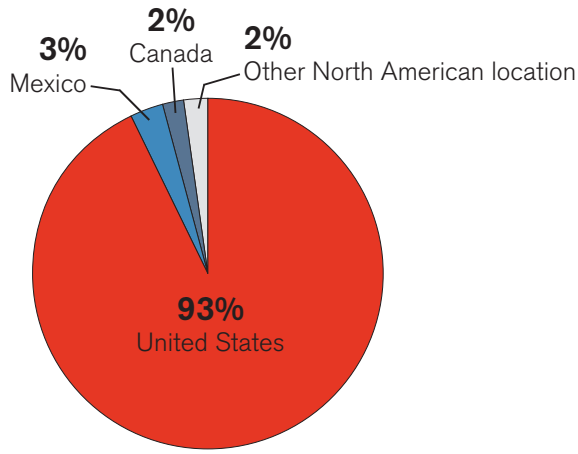
Note: Multiple responses allowed.

Approximately how many people are employed in your entire organization or enterprise?

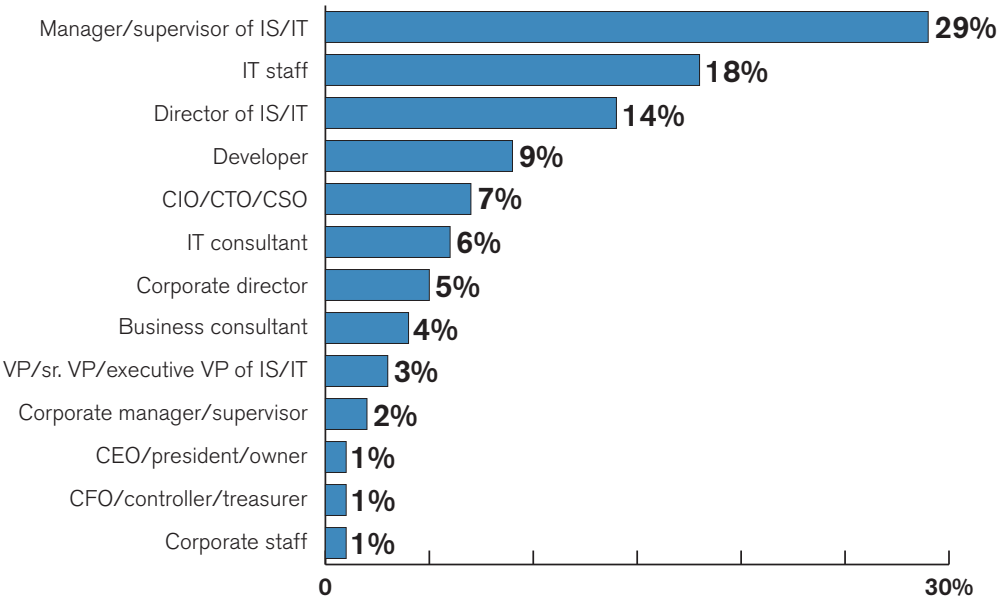


Average company size = 5,443

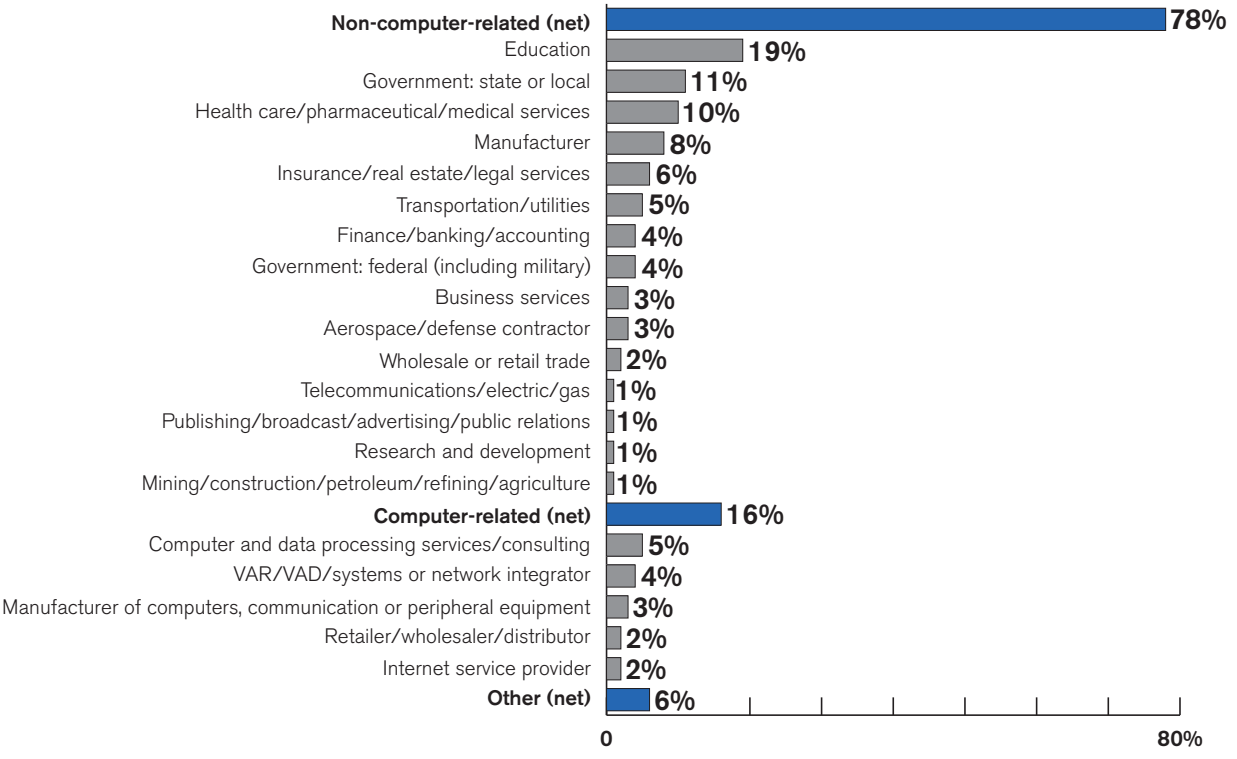
In what country or territory do you currently reside?



Which of the following best describes your primary job function at your organization?



What is your organization's primary business or industry?



Note: Percentages do not equal 100 due to rounding.

Executive summary

With an increase in e-commerce and e-business in recent years, protection of online data has become critical to organizations. Businesses want to have the ability to assure their clients that their Web site communications and transactions are secure. One way of protecting client information is with secure sockets layer (SSL) technology. Most major Web servers have already deployed SSL connections, and SSL is playing a more central and important role in online business activities. SSL certificates allow clients to send confidential information by authenticating the identity of a Web site and enabling encryption technologies. Once SSL technology is in place, information traveling along the connection cannot be tampered with.

Respondents to this research reported an average deployment level of 214 SSL certificates at their organization. Not surprisingly, the most common type of certificate currently deployed is the standard SSL certificate at 86%. Current usage of other types of certificates is lower: wildcard certificates (28%), code signing certificates (20%), extended validation certificates (13%), and unified communication certificates and Adobe CDS certificates (9% each).

Within the next 12 months, 13% of respondent organizations plan to deploy extended validation certificates, followed by code signing certificates (10%) and unified communications certificates (9%).

The importance of a solid validation process of SSL certificates is clear, with more than eight out of 10 respondents rating a reputable validation process as an extremely or very important feature of SSL certificates. Low price is also important to respondents with 63% rating this as extremely or very important. Of lesser importance is validation using just the domain name, showing the importance of organization-validated SSL in order to ensure that not just domain ownership is verified through an automated process, but also to implement a human-based component to verify that the organization is a legitimate business.

The importance of validation also shows when choosing an SSL certificate vendor, again with more than eight out of 10 respondents rating a reputable validation process as extremely or very important. Three-quarters of respondents also feel that a vendor's overall reputation and security expertise are extremely or very important. Although six out of 10 respondents feel that low price is important when choosing an SSL vendor, other factors such as reputation and security expertise rate above low price, even in these rough economic times. These findings suggest that organizations are willing to pay more for a trusted reputation and validation process. In fact, for a standards-based SSL certificate, respondents report that they are willing to pay an average of 9% more for the brand.

However, lower importance ratings for recognized brand (59% rating this feature as extremely or very important), combined with low importance of server gated cryptography as an SSL certificate feature (18% rating this feature as extremely or very important), imply that organizations may not be willing to pay unnecessary premiums for brand names or for certificates supporting browsers over nine years old with weak encryption.

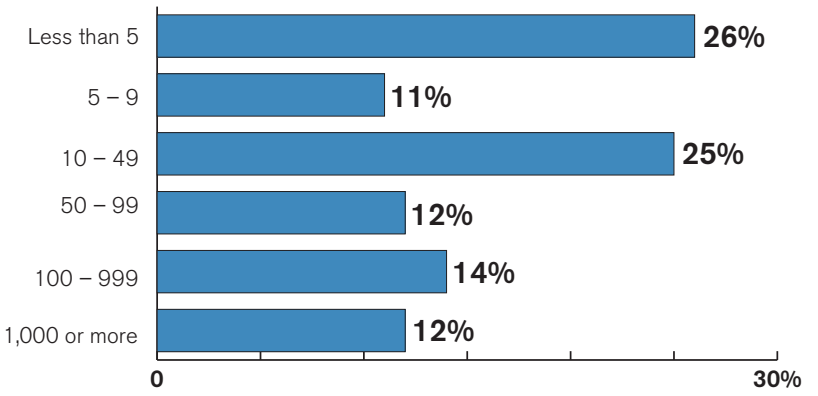
Vendor reputation and security expertise are critical. When asked how important the reputation and security expertise of the SSL certificate vendor they choose is, 82% of respondents rate the reputation and security expertise of the vendor as extremely or very important.

Users conducting online business have become accustomed to certain indicators that their information is protected as it passes through cyberspace. While respondents report that their online users find the yellow lock, the address bar turning green and the name of the SSL vendor important as trust indicators, the yellow lock is reported to be the most important to nearly half of online users, followed by a stringent validation process at 14%.

Number of SSL certificates deployed

On average, respondents report having 214 SSL certificates deployed. Nearly four out of 10 respondents (38%) have 50 or more SSL certificates deployed at their organization.

Approximately how many SSL certificates are deployed in your organization?

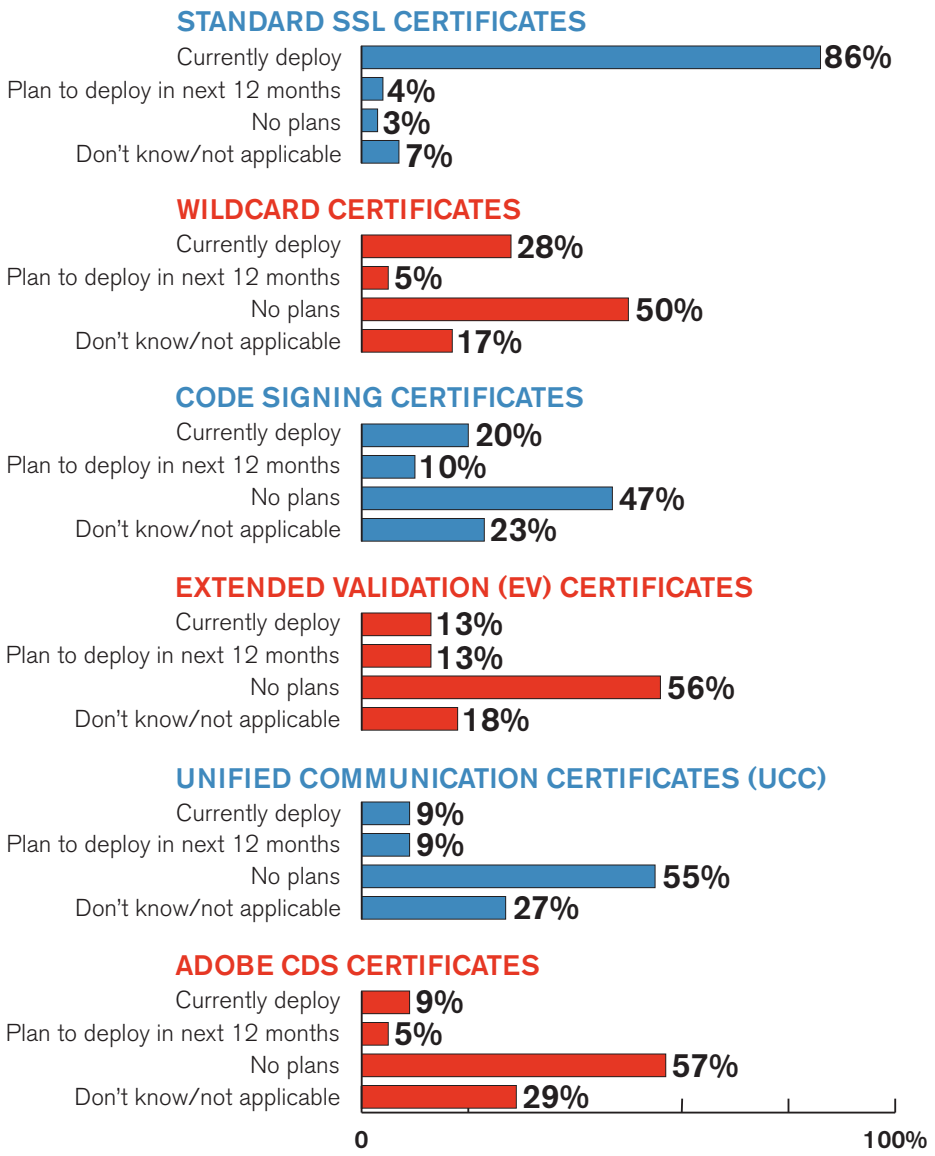


Deployment of different types of certificates

Of the different types of certificates, more than eight out of 10 respondents (86%) currently deploy standard SSL certificates. Current deployment of other types of certificates is lower at 28% for wildcard, 20% for code signing, 13% for extended validation, and 9% for both unified communication and Adobe CDS.

The most common types of certificates that respondents plan to deploy within the next 12 months include extended validation (13%), code signing (10%) and unified communications (9%).

Which of the following best describes your organization's deployment of each type of certificate?

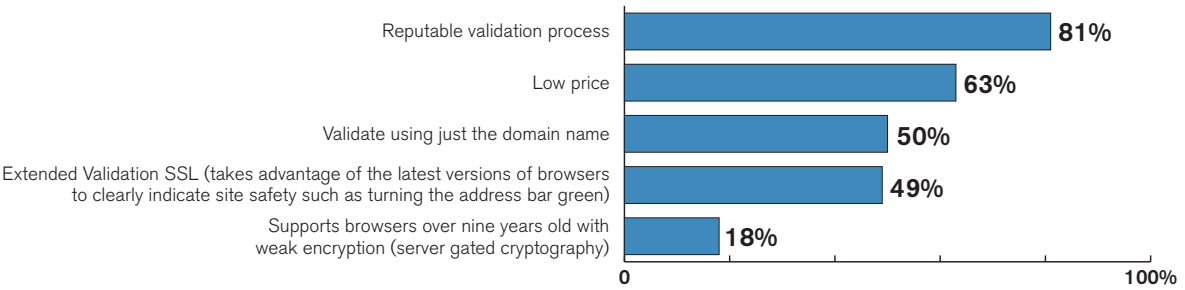


Importance of SSL certificate features

A reputable validation process is the most important SSL certificate feature, with more than eight of 10 respondents (81%) rating this feature as extremely or very important to their organization. Low price is also important with 63% rating this feature as extremely or very important.

It is clear that domain validated SSL certificates are less trustworthy, with only half of respondents (50%) reporting that an SSL certificate validated using just the domain name is extremely or very important. Just under half of respondents (49%) rate extended validation SSL as extremely or very important. Importance of server gated cryptography is low with only 18% of respondents rating support for browsers over nine years old with weak encryption as extremely or very important.

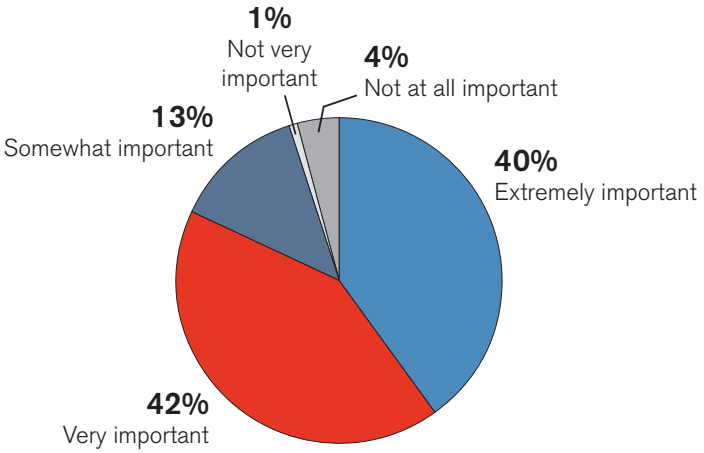
Please rate the level of importance of the following features of SSL certificates to your organization. (Percentages reflect a rating of extremely or very important)



Importance of reputation and security expertise

Reputation and security expertise of SSL certificate vendors is important, with 82% of respondents rating the reputation and security expertise of the vendor they choose as extremely or very important.

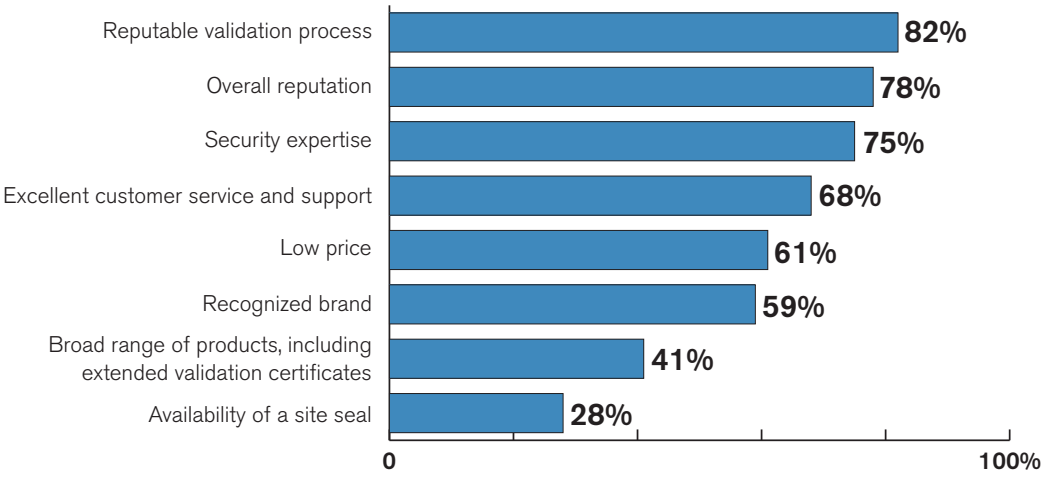
How important is the reputation and security expertise of the SSL certificate vendor you choose?



Importance of factors when choosing an SSL certificate vendor

Respondents cite several important factors when considering SSL certificate vendors. Among the most important are a reputable validation process (82%), overall reputation (78%) and security expertise (75%). With lower importance ratings for recognized brand (59%), combined with low importance of server gated cryptography as an SSL certificate feature (18%), the findings suggest that respondent organizations may not be willing to pay unnecessary premiums for brand names or for certificates using server gated cryptography that are only necessary for a small number of users.

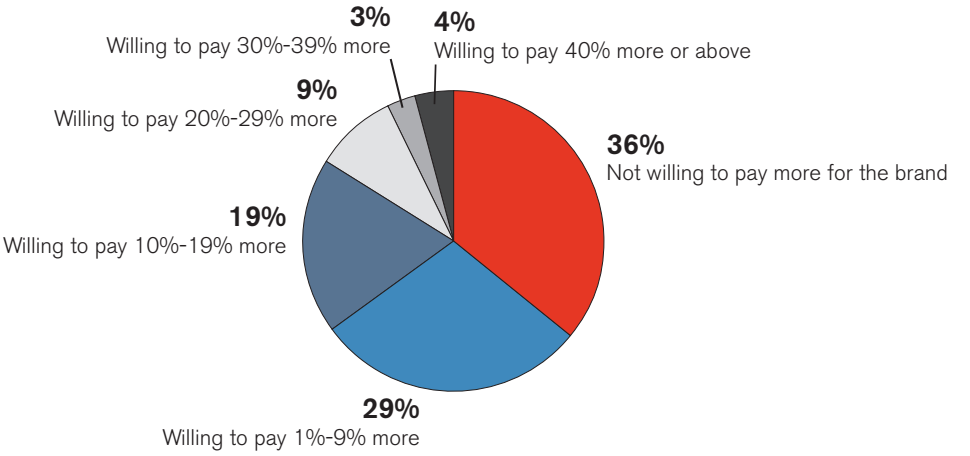
Please rate the level of importance of the following factors when choosing an SSL certificate vendor. (Percentages reflect a rating of extremely or very important)



Willingness to pay for the brand

For a standards-based SSL certificate, respondents indicate that their organization is willing to pay an average of 9% more for the brand. While six out of 10 respondents report that low price is important when choosing an SSL vendor, other factors, including reputation and security expertise, rate above low price, even with the state of the economy today. This data suggests that organizations are willing to pay more for a trusted reputation and validation process.

For a standards-based SSL certificate, how much more is your organization willing to pay for the brand?

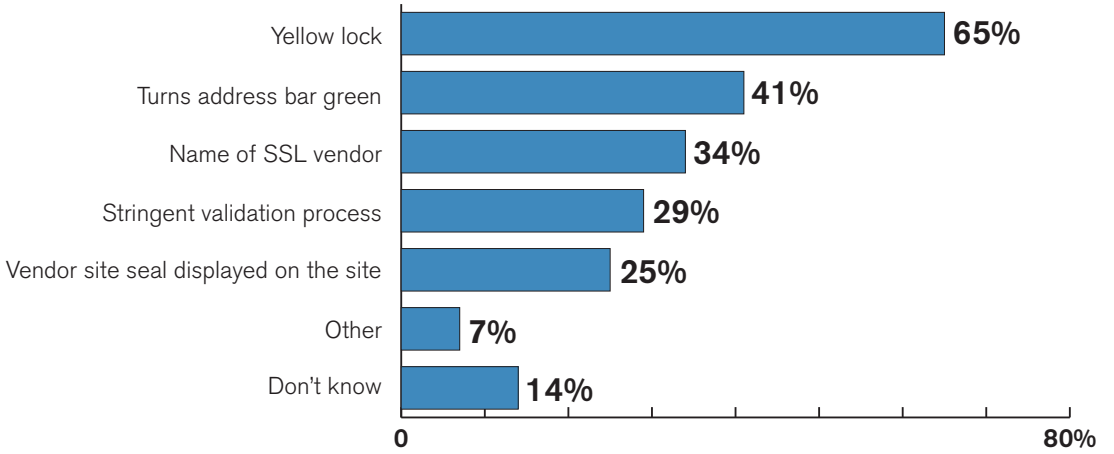


Trust indicators for online users

Online users have become accustomed to certain security features that ensure their information will be protected. One such trust indicator is the yellow lock shown on protected Web sites. Two-thirds of respondents (65%) report that their organization's online users think the yellow lock is important as a trust indicator. Other top trust indicators include turns address bar green (41%), name of SSL vendor (34%), stringent validation process (29%) and vendor site seal displayed on the site (25%).

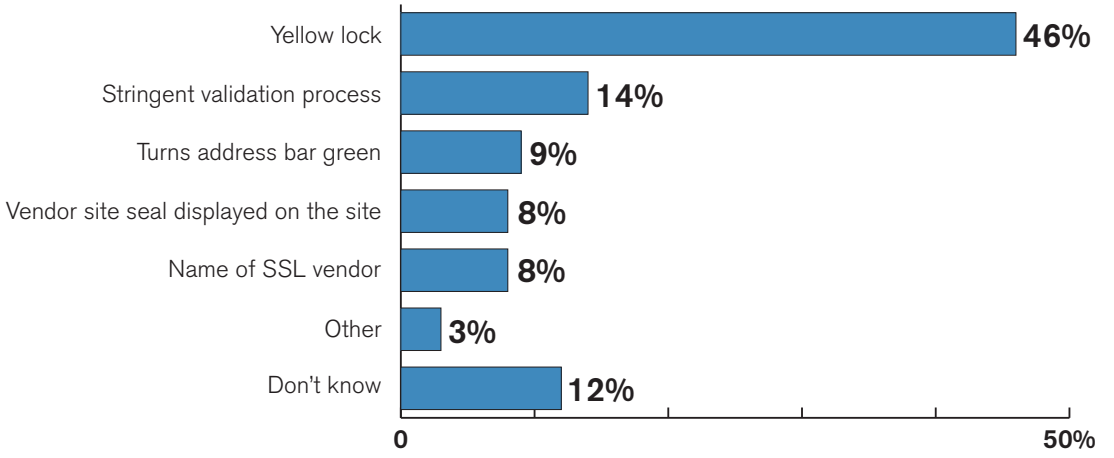
Nearly half of all respondents (46%) think that the yellow lock is the most important trust indicator. The yellow lock is distantly followed by a stringent validation process (14%).

Which of the following trust indicators do your organization's online users think are important?



Note: Multiple responses allowed.

Which one of the following trust indicators do your organization's online users think is the most important?



Conclusion

Protecting the confidential transactions of e-commerce and e-business is becoming increasingly important. In fact, overall reputation and security expertise are the most important factors when choosing vendors that supply risk-reducing products and services. Even in these tough economic times, organizations are willing to sacrifice a lower price for reputation and expertise. With a reputable validation process being the most important SSL certificate feature, organizations will be looking toward SSL vendors with a solid validation process, including organization validated SSL, to ensure that not just domain ownership is checked but also to verify that the organization is a legitimate business.

So what does all this mean for your organization? Basically, your organization can use responses from this survey as a benchmark for how your peers are addressing these issues. If your organization is not currently making certificate purchase decisions with the reputation of the vendor, the validation process and the value you are receiving for the price in mind, you need to begin to address these areas. It's important that the solution you seek enables your organization to maximize the security of its digital transactions in a cost-effective manner, without paying unnecessary premiums for features such as server gated cryptography that are only necessary for a small number of users.