2013 Online Trust Honor Roll & Online Trust Index

Independent Audit of Best Practices In:

- Domain, Brand & Consumer Protection
- Site, Server & Infrastructure Security
- Data Protection, Privacy & Transparency

June 5, 2013

OTA
Online Trust Alliance

Table of Contents

EXECUTIVE SUMMARY

As the threat level of cybercrime, state sponsored cyber terrorism, hactivism and online fraud reaches all-time highs, it is becoming more critical for online brands and service providers to take proactive measures to protect their users and brands from threats that undermine online trust and confidence. Compounded by heightened privacy concerns regarding data collection and usage, businesses are fast approaching a critical juncture. Businesses that fail to move from a compliance driven culture to one of stewardship risk disenfranchising consumers and validating the need for increased regulatory oversight.

Over the past four years, the Online Trust Alliance (OTA) has conducted the annual Online Trust Honor Roll audit. The 2013 Honor Roll examined the brand protection, security and privacy protection practices of over 750 websites, including the 2013 Internet Retailer Top 500 (IR 500), leading financial institutions (FDIC 100), social networking sites and OTA member companies.[1] With publically disclosed criteria, sites were analyzed based on the adoption of fourteen industry accepted best practices, open standards and privacy practices which comply with industry norms, criteria and best practices advocated by the Federal Trade Commission and the National Institute of Standards and Technology.

The Honor Roll recognizes leading online companies' efforts to enhance the security and privacy of user's data and their adoption of leading self-regulatory practices, polices and technologies. The report represents a holistic view of widely accepted best practices to help secure consumer data, enhance user privacy and protect brands online.

The criteria used in the Honor Roll are highly relevant to the security and privacy practices companies must implement to address these vulnerabilities. OTA has identified and evaluated three key areas of competency to maximize online trust:

- Domain, Brand & Consumer Protection
- Site, Server & Infrastructure Security
- Data Protection, Privacy & Transparency

It is important to recognize that a company's most valuable assets – brand and integrity – take years to build and only seconds to collapse. This can result in the erosion of consumer confidence and trust, a significant part of a company's value proposition and competitive advantage. Look no further than the daily headlines for evidence that external and internal threats are commonplace (2,644 reported breaches worldwide in 2012, exposing 267 million records), and will continue to be so if companies do not implement responsible security practices.

OTA's methodology has expanded over the years to accommodate new technologies and processes that are critical to a business's infrastructure as well as the organic growth of big data as a result of the evolution of the digital ecosystem. While initial reports focused almost exclusively on email authentication and Extended Validation SSL certificates

[1] Raw data is from the Internet Retailer Top 500 Guide (http://www.internetretailer.com/top500/), a ranking of the largest North American e-retailers by online sales, produced by Vertical Web Media, publisher of Internet Retailer magazine.

(EV SSL), the 2012 report was significantly expanded to include SSL implementation and privacy policy analysis.

The2013 criteria has been expanded to include the examination of certificate bit SSL Keys, Domain Locking, honoring of Do Not Track (DNT), and a revised weighting of email authentication scores to reflect current best practices. The report primarily focuses on consumer-facing sites that have been most frequently targeted by cybercriminals and the associated deceptive business practices of phishing, account takeovers, breaches and domain/email spoofing.

To qualify for the Honor Roll, companies had to receive a composite score of 80% or more of the available points and score at least 55% in the three major categories of brand/domain protection, site security, and privacy policies and practices. The minimum scoring requirement was instituted in 2013 recognizing sites are built on a "chain of trust" that is only as strong as its weakest link.

The primary goal for the Honor Roll and Online Trust Index (OTI) is to recognize outstanding leadership by highlighting companies as "North Stars" for others to follow. Qualifying to the 2013 Honor Roll reflects the commitment to best practices which aid in the protection of online trust and consumer confidence in online services. A secondary goal is to promote best practices and provide prescriptive tools and resources to aid companies in enhancing their security, data protection and privacy practices. Introduced in 2012, the OTI is a composite average score to provide sector comparability and benchmark reporting.

While OTA does not endorse individual sites, consumers are encouraged to consider that a site has qualified for the Honor Roll based not only on the criteria outlined in this report, but also on other reputational data. Users should consider ratings from organizations such as the Council of Better Business Bureau and other independent online reviews including organizations who participate in self-regulatory and safe harbor programs such as the Network Advertising Initiative, (NAI).

This year the Honor Roll report and associated Appendices have been published separately. The Appendices include:

- List of Honor Roll recipients in all sectors
- Sector definition and summary analysis by sector
- Methodology details
- Description of the scoring components
- Background information on key technologies including email authentication, DMARC and EV SSL
- History of the OTA Honor Roll
- Resources

ONLINE TRUST HONOR ROLL HIGHLIGHTS

Thirty-two percent of companies qualified for the Honor Roll this year, vs. 30% last year, even though the criteria was tightened and the bar raised in several areas, (232 of 709 analyzed [2]). Such changes cover all key categories including email authentication, site security and privacy requirements. In addition, to qualify sites had to exceed 55 points in each of the three major categories. Nearly half of the companies (122) achieved Honor Roll status for the second year in a row. Conversely, 46 companies who made the Honor Roll in 2012 did not qualify for the 2013 Honor Roll. The results highlight the need to continually manage, monitor and maintain a site's, security and privacy policy and practices. A complete list of Honor Roll recipients by sector is available in Appendices A-D.

New this year is recognition of the Internet Retailers 500 top 10 Honor Roll scoring retailers including American Greetings who received the highest overall score.[3] These companies range in size based on the IR 500 rankings from number one (Amazon) to number 453 (Books-A-Million), validating that the prescribed best practices can be implemented by companies of any size. Though 26% of the IR 500 made the Honor Roll, 74% have not fully adopted best practices, exposing users to security and privacy threats. Of the non-qualifying IR500, 52.8% received failing grades in one or more of the key categories.

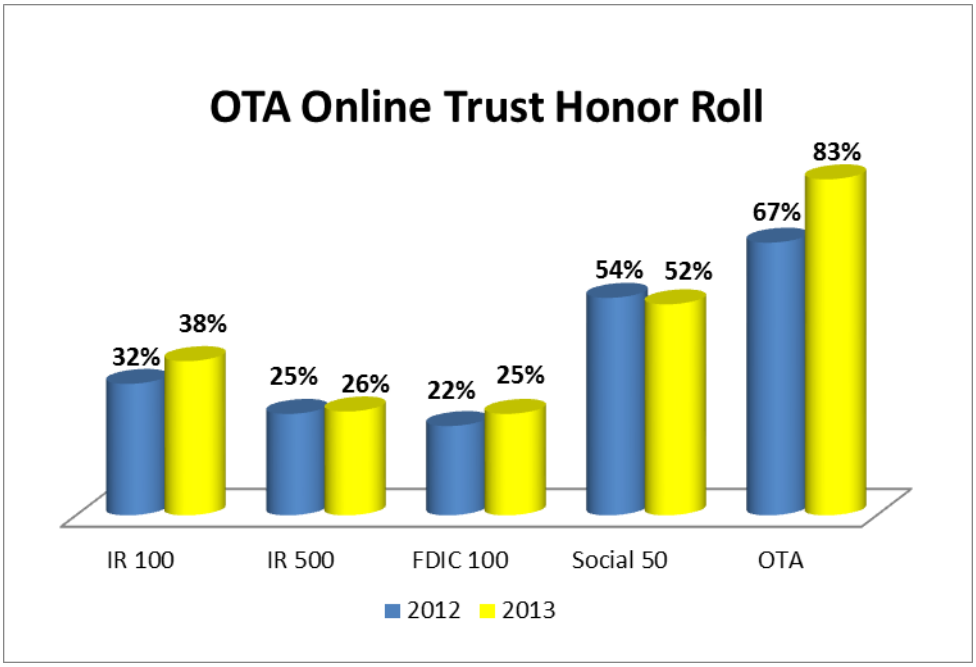

Figure 1 – Percent of Sector Achieving 2013 Honor Roll Status

[2] The number of companies analyzed for the report varies due to an overlap between OTA members and other sectors, the Federal 50 is excluded from Honor Roll and privacy scoring, some sites do not have SSL and therefore cannot be scored, and five social sites have privacy policies in a foreign language and could not be accurately assessed. For the purpose of the analysis, a total of 759 sites were analyzed for most of the component scores that covered all sectors, 742 sites were analyzed for SSL scores, 709 sites were assessed for Honor Roll qualification, WHOIS and Domain Locking, and 704 sites were analyzed for privacy scores.

[3] Due to scoring ties, the top 10 includes 12 companies.

As shown in Figure 1, OTA members had the largest rise in percent of companies making the Honor Roll (from 67% last year to 83% in 2013), followed by the top 100 online retailers (from 32% to 38%). These improvements were primarily driven by higher SSL scores, indicating increased focus on site security and privacy policies.

Eighty-three percent of OTA members, which are comprised of leaders in ecommerce, social media, online marketing, identity theft protection and technology services, qualified for the 2013 Honor Roll. This was higher than all other segments, reflecting their involvement in development and adoption of voluntary best practices and commitment to adopt them when joining OTA.

The slight decline in Honor Roll achievement for social sites is primarily due to an increase in the number of sites audited from 27 in 2012 to 50 in 2013. Also impacting the score was the broadening of the category to include top image sharing, blogging, gaming and dating sites. A year-over-year comparison using the same social networking sites shows that 57% made the Honor Roll in 2013 vs. 54% in 2012. In general, social sites have strong scores due to their reliance on all three core aspects of the scoring – email, site security and privacy.

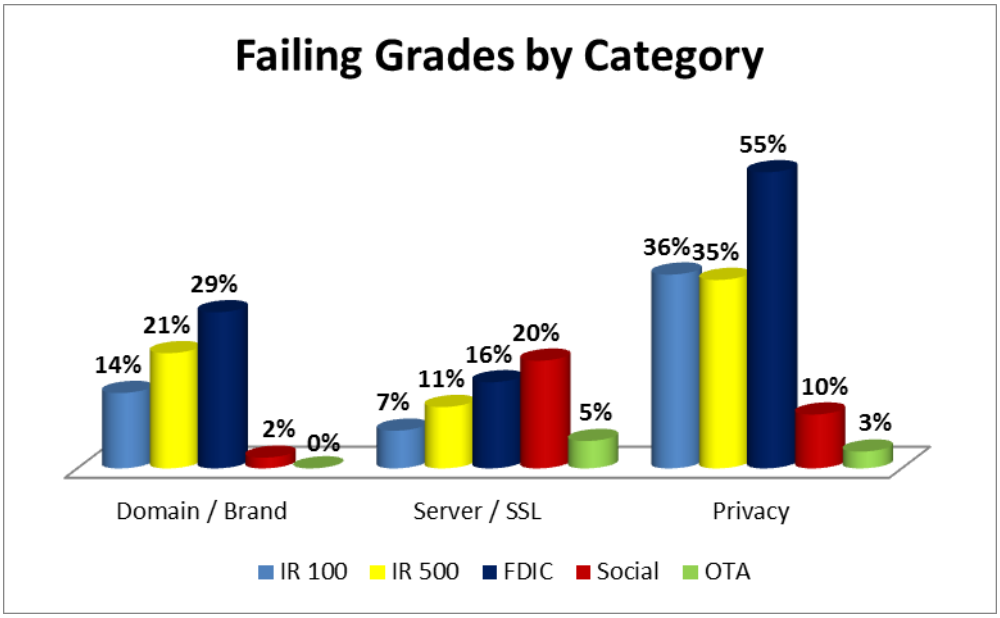

Figure 2 – Percent of Companies with Failing Grade by Sector and Category

With the introduction of a minimum score required in each major category to qualify for this year's Honor Roll, it is insightful to look at failing grades across sectors to focus on major areas for improvement. Figure 2 shows the percentage of companies in each sector that had a failing grade in that category.

The FDIC 100 had the most failing grades (71%) in one or more areas largely attributed to low scores due to privacy practices that share data with unaffiliated third parties. Domain and brand protection was also a weakness for the FDIC 100; primarily due to lack of DKIM support across top level domains and consumer email sub-domains.

Internet Retailers, while scoring higher than the FDIC 100, have similar top rated deficiencies including sub-optimal privacy policies and practices and email authentication. The primary area of potential improvement for social sites is server/SSL security, where 20% of the sites had failing grades.

The Online Trust Index (OTI), which was added to the report in 2012, is calculated for each consumer-facing sector, including online retailers, the FDIC 100, and social sites. Consistent with past analysis, OTA members are also tracked. Providing comparability across sectors and a baseline for future benchmark reporting, the OTI has been normalized as an average trust score on a scale from 1 to 100.

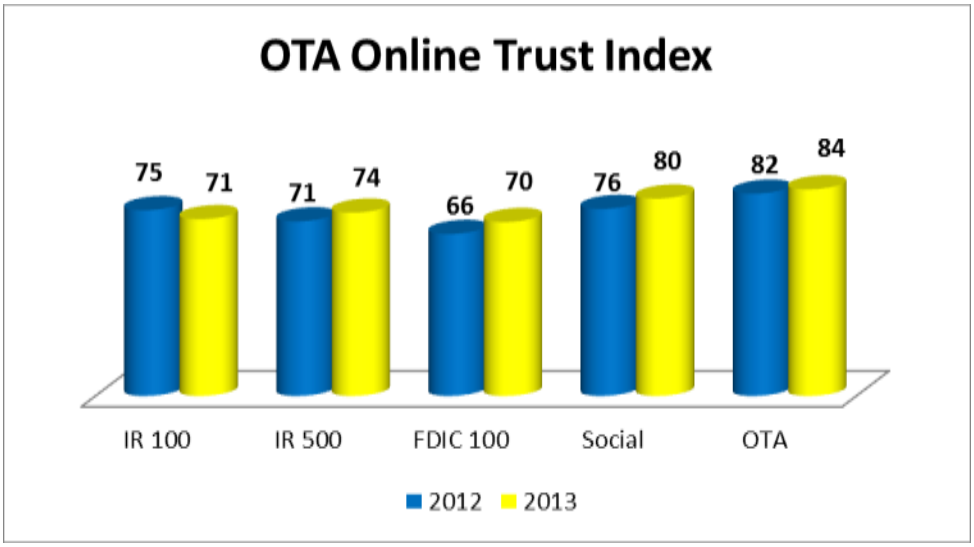

Figure 3 - Online Trust Index by Sector

OTI scores improved across all sectors with the exception of the top ranked Internet Retailer 100 largely due to shifts in scoring for email authentication. In 2013, a heavier emphasis was placed on implementing SPF and DKIM at the top-level domain to maximize brand protection. In addition, reflecting the broad adoption since the draft specification was released in January 2012, DMARC support was moved from bonus points to a component of the baseline score.

INDIVIDUAL BEST PRACTICES HIGHLIGHTS

Domain, Brand & Consumer Protection

- **Email Authentication (SPF & DKIM)** – adoption of email authentication continues to rise across all sectors with the Social 50 and OTA scoring nearly 100%.
    - The largest increase was in the adoption of both SPF and DKIM, which rose 10%-20% in nearly every sector (e.g., IR 100 adoption of both rose from 56% to 76%; FDIC 100 adoption of both rose from 34% to 49%).
- **Domain-based Message Authentication, Reporting & Conformance (DMARC)**
    - Adoption, though still low by comparison to SPF or DKIM, grew significantly (especially in the FDIC 100, which had a 13-fold increase). Every sector now has an organization asserting a "reject" or "quarantine" policy to email receivers.
- **Domain Locking** – New to this year's report, the audit now examines whether companies prevent transfer of domains in their domain registration.
    - The vast majority of companies (98%) lock their domains.

Site, Server & Infrastructure Security

- **SSL Server Configuration**
    - Average scores improved 6-10 points in all sectors, even though criteria was tightened to cap scores based on vulnerability to common attacks. Overall, the average across sites with SSL rose to 84.6 from 76.7 last year.
    - The IR 100, IR 500, FDIC 100 and OTA member sites scored within five points ranging from 82 to 87 with the Federal 50 falling short at 73.2 and OTA members taking the lead at 87.1.
- **Extended Validation SSL Certificates (EV SSL)** – Worldwide use grew more than 28% this year to more than 74,000 deployed certificates.
    - The FDIC 100 leads adoption with 60% due to their need to communicate trust to users conducting financial transactions on their sites. They are followed by the IR 500, with a 35% adoption rate.
- **Always On SSL (AOSSL)** – A more thorough analysis was done to determine whether sites were securing all pages.
    - The FDIC 100 leads adoption with 61%, reflecting their need to ensure a secure environment for their users.
    - There is modest use of AOSSL in the Federal 50 (9%), Social 50 (10%), and OTA members (9%).

- **2048-Bit Key or Elliptic Curve Cryptography (ECC) Certificates** – Added this year, to support the upcoming NIST requirement effective January 2014.
    - Most sites have already moved to a 2048-bit key (and some to a 4096-bit key) in advance of the NIST requirement. Adoption ranged from 85% (Federal 50) to 91.7% (OTA members).
    - ECC adoption was not measured as a result of its recent release, but is expected to accelerate as sites replace expiring certificates.
- **Domain Name System Security Extension (DNSSEC)**
    - Adoption is clearly concentrated in the Federal 50 with 88%, though there is some adoption (8%) amongst OTA members.

Data Protection, Privacy & Transparency

- **Privacy Policy & Third Party Tracking**
    - Scoring was tracked for all sectors but the Federal 50. The overall average across all sampled sites was 66.5, a slight increase from the overall average of 64.7 in 2012.
    - For consumer-facing sites, the Social 50 leads with an average of 76.2 followed by the IR 500 at 64.4 and the FDIC 100 at 61.1, highlighting room for improvement in those sectors.
- **Honoring of Do Not Track Browser Settings (DNT)** – New in 2013.
    - Though it is important to honor users' browser requests, this is a nascent area with only 1 adopter (Twitter) across all sampled sites. It is expected once the DNT standard and policies are ratified by the W3C, adoption and public support will accelerate.
- **Public vs. Private WHOIS registration** – Public registration is important for transparency of site ownership management and contact information.
    - The vast majority of sites (97%) have public domain registrations. The largest concentration of private registration was found in the IR 500 (4.2%).
- **Data Breach & Loss Incidents**
    - Fifty-two of the sampled organizations (6.9%) had a breach incident in the last two years. The IR 500 had the lowest rate (2.8%) of breaches. All other sectors were in the 10-15% range.
- **FTC / State Settlements**
    - Eight of the sampled organizations (1.1%) had FTC suits or settlements in the last two years. These were concentrated in the Social 50 (8%) and IR 100 (5%).

SECTOR HIGHLIGHTS

See Appendix E for a complete definition of each sector.

Internet Retailer 500

- Strong growth in overall use of SPF (from 63% to 79%) and both SPF and DKIM (from 43% to 56%), but there is still room for improvement in use of DKIM at top-level domains to maximize brand and consumer protection.
- Received the highest SSL score (85.3) amongst consumer-facing sectors, though their privacy scores reflect the need for improvement (64.4) as they lag other sectors.

FDIC 100

- Led all sectors by far in EV SSL adoption (60%) and AOSSL adoption (61%), contributing to their high overall SSL score.
- Continued growth in overall email authentication – 77% use either DKIM or SPF (vs. 69% last year), 49% uses both (vs. 34% last year) – though these numbers still lag other sectors.
- Low privacy scores for many financial institutions prevented them from qualifying for the Honor Roll. Part of the reason is their privacy policies stating they share data by default with unaffiliated third parties.

Social 50

- Top consumer-facing sector for percent of companies making the Honor Roll (52%) and OTI scores (80).
- Near the top in adoption of email authentication (98% use either DKIM or SPF, 72% use both), and early adopters of DMARC (22% have already adopted, 64% of them with directives to reject or quarantine failed messages).

OTA Members

- Highest adoption of email authentication (100% support either DKIM or SPF, 69% support both), and strongest early adopters of DMARC (42%).
- Highest overall SSL score (87.1) and adoption of 2048 bit certificates (91.7%).

Federal Government 50

- Continued strong growth in use of email authentication (72% of sites use SPF or DKIM, up from 58% last year; 20% of sites use both SPF and DKIM, up from 10% last year), but still room for improvement.
- Primary adopter of DNSSEC (88% - the next highest sector is 8%), reflecting support of the White House Office of Management and Budget directive.
- Lagging in SSL scores (Federal 50 averaged 73.2 vs. overall average of 85.0).

OVERVIEW & BACKGROUND

This is the fourth consecutive year OTA has published the Online Trust Honor Roll report, building on the first OTA score card introduced in 2005. The sectors evaluated include; internet retailers, financial services, federal government agencies, social sites and OTA's own membership.

This report represents a composite analysis of a wide variety of factors evaluated across three major categories including: Domain, Brand & Consumer Protection; Site, Server & Infrastructure Security; and Data Protection, Privacy & Transparency. The key sectors represent more than 750 domains – and the analysis is a "snapshot in time." Sampling and analysis was conducted between April 21 and May 20, 2013 (details can be found in Appendix F, "Methodology"). The factors are weighted and scored based on the impact they have on email safety, brand protection, website security, consumer transparency, and overall best practices that will distinguish an organization and brand from a business and consumer perspective. Results are used to assess each organization's qualifications for the OTA Honor Roll as well as to compare sectors via an Online Trust Index (OTI) which tracks key sectors' adoption of best practices on a normalized scale of 1-100 points.

Sectors Evaluated:

- Internet Retailer 100 (IR 100)
- Internet Retailer 500 (IR 500)
- FDIC Top 100 Banks (FDIC 100)
- Top 50 Federal Government (Federal 50)
- Top 50 Social Sites (Social 50)
- OTA Members

As in previous years (see Appendix J for Honor Roll Milestones), the criteria for this year's report are indicative of the most current best practices supported by OTA, other organizations and government agencies. The criteria were adjusted to address the constantly evolving threat environment and the need for all sites to continually monitor their security and privacy practices.

Enhancements to the 2013 Honor Roll report reflect three key changes:

- The weighting of email authentication shifted to focus on the importance of adoption of both SPF and DKIM at the top-level corporate domain – addressing the risk of spearphishing.
- Domain-based Message Authentication, Reporting & Conformance (DMARC) is now a baseline criterion rather than a bonus score.
- Secure Socket Layer (SSL) analysis evolved to cap scores for sites vulnerable to current attack vectors, and bonus points were added for sites who have adopted 2048-bit certificates (vs. 1024 bit) that will be a National Institute of Standards and Technology (NIST) requirement by January 2014.

Key factors of the analysis are noted below (a detailed description of each item can be found in the Appendix G, "Components of the Composite Score").

To qualify for the Honor Roll, company sites must receive a composite score of 80% or better AND score at least 55 in each of the three categories. The Honor Roll evaluates a total of fourteen criteria in the three major categories;

DOMAIN, BRAND & CONSUMER PROTECTION

- Email Authentication (SPF & DKIM)
- Domain-based Message Authentication, Reporting & Conformance (DMARC)
- Domain Locking

SITE, SERVER & INFRASTRUCTURE SECURITY

- Secure Sockets Layer (SSL) Server Configuration
- Extended Validation SSL Certificates (EV SSL)
- Always On SSL (AOSSL)
- 2048 bit key or Elliptic Curve Cryptography (ECC) Certificates
- Domain Name System Security Extension (DNSSEC)

DATA PROTECTION, PRIVACY & TRANSPARENCY

- Privacy Policy
- Third Party Tracking on Site (included in Privacyscore analysis)
- Honoring of Do Not Track Browser Settings (DNT)
- Public vs. Private WHOIS registration
- Data Breach & Loss Incidents
- FTC / State Legal Settlements

While there is no silver bullet or guaranteed security, applying operational and security discipline and implementing the prescribed best practices can minimize the attack surface and help protect consumers, data and critical infrastructure from abuse.

Organizations that adopt these best practices will realize brand differentiation and demonstrate to their customers, shareholders and regulators that they are prioritizing their accountability and commitment to consumer protection. As stewards of data and consumer trust, it is both an opportunity and obligation.

DOMAIN, BRAND & CONSUMER PROTECTION

Email authentication (SPF and DKIM) and its companion DMARC technology combined with domain locking, provide organizations with a mechanism to enhance the protection of their brands and consumers from commonly used deceptive ploys. Email authentication allows senders to assert details about who is authorized to send email on their behalf. DMARC adds a policy assertion providing receivers direction on how to handle mail that fails authentication. Domain locking ensures that domain ownership cannot be transferred without the owner's permission, further helping to protect a site's brand from abuse.

Combined, all three provides receivers increased accuracy on email delivery. The benefits help prevent spoofed email from being delivered to the inbox; enhances integrity of the domain and helps to prevent fraud including identity theft and account takeover.

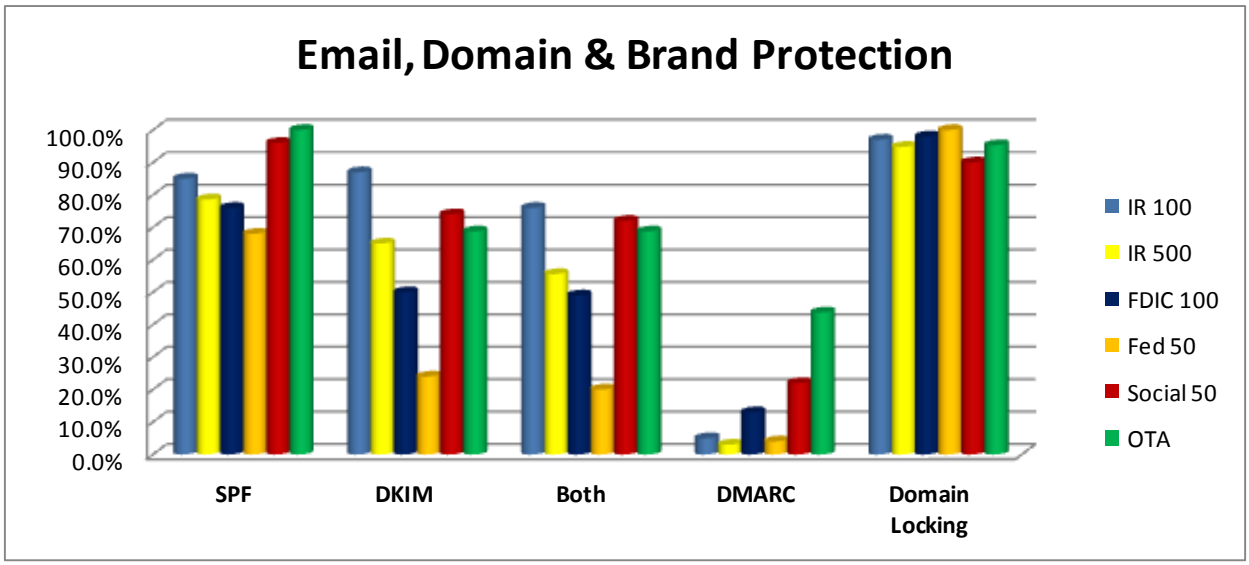

Figure 4 – Email Authentication, DMARC, Domain Locking Adoption by Sector

EMAIL AUTHENTICATION

In early 2004, several initiatives emerged to help address the threats of deceptive email, phishing and spam. Working through the standards community, and with broad industry and business input, two key email authentication technologies emerged that allowed senders to be verified: Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). Organizations worldwide have found that adoption of both SPF and DKIM, versus utilizing either independently, best enables receivers to detect and block forged and malicious email, while reducing the risk of false positives from mail being forwarded or sent to mailing lists.

Since 2005, OTA has published reports highlighting email authentication best practices and the respective value proposition to brand and consumer protection.[4] Each successive report

[4] https://otalliance.org/news/releases/F500_reportcard.html and https://otalliance.org/news/releases/OTA_414reportcard.html

has included additional detail about adoption of these key authentication technologies across a variety of industry sectors.

As seen in Figure 4, adoption of SPF ranges from 68% to 100%, while DKIM adoption ranges from 24% to 87%. The IR 100, Social 50 and OTA members lead in sites adopting both SPF and DKIM – the prescribed best practice – ranging from 69% to 76%. This corresponds with their reliance on email as a primary communications channel with their customers. The Federal 50 lags in all categories.

DMARC adoption, just 18 months after its announcement, is highest for OTA members and the Social 50. DMARC adoption is expected to grow significantly across all sectors over the next two years as ISP support grows and corporate mail systems are updated.

Figure 5 shows the growth in adoption for sites utilizing either SPF or DKIM over the last four years, while Figure 6 shows the adoption rate for sites supporting both SPF and DKIM.

2013 Domain & Brand Protection Either DKIM or SPF				
	2010	2011	2012	2013
IR 100	76%	84%	97%	96%
IR 500	54%	65%	91%	88%
FDIC 100	55%	59%	69%	77%
Fed 50	32%	38%	58%	72%
Social 50		92%	96%	98%
OTA Members	88%	95%	99%	100%

Figure 5 – Adoption of Either SPF or DKIM, 2010-2013

2013 Domain & Brand Protection Both DKIM and SPF				
	2010	2011	2012	2013
IR 100	24%	42%	56%	76%
IR 500	14%	23%	43%	56%
FDIC 100	22%	23%	34%	49%
Fed Sites	2%	4%	10%	20%
Social 50	-	28%	63%	72%
OTA Members	36%	44%	59%	69%

Figure 6 – Adoption of Both SPF and DKIM, 2010-2013

From the figures above, it can be seen that overall adoption continues to grow with several sectors approaching 100% adoption of either SPF or DKIM. The largest growth in this category was made by the Federal 50, which grew from 58% to 72%, but it still lags all other sectors. Adoption of both SPF and DKIM made great strides across all sectors in the last year, led by the IR 100 which grew from 56% to 76%. Support of this best practice allows receivers to make enhanced and more accurate decisions about the validity of email being sent.

SPF ADOPTION ANALYSIS

Overall SPF adoption continues to grow, as shown in Figure 7. New this year is the inclusion of SPF adoption at the subdomain level (vs. just the top-level domain, or "TLD"[5]). While the primary focus is to implement SPF at the TLD to protect against spearphishing[6] and forged email, it is also important for email marketers and brand owners to authenticate all subdomains. The IR 100 and Federal 50 both grew 10% in absolute rate of adoption at the top-level domain, from 67% to 77% and 50% to 60% respectively. Federal 50 growth reflects support of the Federal CIO Council, White House Office Management & Budget (OMB), and the U.S. Department of Homeland Security. Sectors near the 100% adoption level dropped slightly due to changes in OTA membership or expansion of the category (Social 50). Factoring in SPF at the subdomain level shows an increase in adoption rate of 8-14% for the IR 500, FDIC 100 and Federal 50.

2013 Domain & Brand Protection SPF Adoption					
	2010	2011	2012	2013	
	Top Level Domains	Top Level Domains	Top Level Domains	Top Level Domains	Any SPF
IR 100	76%	84%	67%	77%	85%
IR 500	54%	65%	63%	69%	79%
FDIC 100	55%	59%	60%	62%	76%
Fed 50	32%	38%	50%	60%	68%
Social 50	-	92%	96%	94%	96%
OTA Members	88%	95%	99%	98%	100%

Figure 7 - SPF Adoption, 2010-2013

It is critical to implement SPF (and DKIM) on all domains used by an organization to help prevent abuse by cybercriminals who prey on any user-recognizable domain. Organizations should inventory all outgoing mail streams (whether sent and managed in-house or by a third party), and implement email authentication across all domains and subdomains.

Often overlooked are domains that never send legitimate email which may resolve to the top level or web site domain. Site owners need to publish SPF and DMARC records to provide direction to receiving parties to block all such mail which may be purported to come from domains.

[5] The Top Level Domain (TLD) is what is associated with the home page and most recognizable to the user. For example, OTA's TLD is https://otalliance.org, with subdomains of email.otalliance.org and list.otalliance.org. The use of OTA's TLD is generally most recognizable and at risk for potential abuse.

[6] Spearphishing is malicious email that is targeted for a specific individual or small group of individuals, usually for the purpose of accessing their credentials or planting malware on their computer to gain additional access within the organization. Spearphishers often pose as employees or business partners of the organization under attack.

DOMAINKEYS IDENTIFIED MAIL (DKIM) ADOPTION ANALYSIS

Overall DKIM adoption, shown in Figure 8, grew significantly again this year, from 46.3% to 65.5%, a 41% increase. Adoption increased in nearly every sector, led by the Social 50, which grew from 63% to 74%, a 17% increase. The IR 100 leads all sectors with 87% adoption, followed by the Social 50 with 74% adoption.

DomainKeys Identified Mail - Adoption Analysis						
	2010	2011	2012	2013		
	Any DKIM	Any DKIM	Any DKIM	Top Level Domains	Sub Domains	Any DKIM
IR 100	37.0%	55.0%	82.8%	**26%**	**81%**	**87%**
IR 500	22.8%	33.4%	69.5%	**18%**	**58%**	**65%**
FDIC 100	29.0%	34.4%	44.0%	**30%**	**38%**	**50%**
Fed 50	4.0%	6.0%	18.0%	**22%**	**6%**	**24%**
Social 50	-	52.0%	63.0%	**62%**	**42%**	**74%**
OTA Members	22.0%	34.5%	57.1%	**58%**	**28%**	**69%**

Figure 8 - DKIM Adoption, 2010-2013

Most of this increased adoption is at the subdomain level, and is driven by use of DKIM in marketing email managed by third parties. Unfortunately, this practice provides little if any domain and consumer protection from spoofed email – adoption at the TLD lags significantly in most sectors, and the year-to-year growth rate is much smaller. The Social 50 is a clear leader amongst consumer-facing sectors, with 62% adoption at the TLD. To maximize brand and consumer protection, DKIM signing needs to be extended to both the TLD and subdomains.

DOMAIN-BASED MESSAGE AUTHENTICATION, REPORTING & CONFORMANCE (DMARC)

DMARC creates *consistency* by leveraging the best of SPF and DKIM; *visibility* by reporting on how receivers process inbound email; and *policy* so senders can declare how to process unauthenticated email. As a result, DMARC is now a baseline scoring component in the composite analysis previously scored as bonus points in 2012.

The key value and benefits of DMARC can be summarized as follows:

- **Policy Assertion.** Senders can specify how they want receivers to treat messages that fail authentication (no action, quarantine or reject), which they can progressively tighten as they become more confident in the accuracy of their authentication implementation. In an ideal scenario, senders that fully utilize DMARC can advise receivers to block all unverified messages from their domains, thus helping to prevent direct-spoof phishing attacks on those domains.

- **Feedback.** Senders can also request reports from receivers on messages that pass or fail DMARC checks, which allows the sender to optimize their outbound authentication and receive important data on phishing attacks against their domain.

DMARC ADOPTION ANALYSIS

DMARC.org released its first year adoption findings in January 2013, reporting that 60% of the world's consumer email boxes from leading ISPs (nearly 2 billion accounts) now support DMARC, thus providing added protection for email from senders who have adopted email authentication and have published DMARC records. Adoption by large email receivers helps address the "chicken and egg" problem often seen in adoption of new technologies – senders are reluctant to adopt DKIM if they do not see support by a critical mass of receivers. With significant adoption by receivers, senders can realize the value of DMARC quickly.

DMARC Adoption			
	2012	2013	
	Record	Record	R or Q
IR 100	2.0%	5.0%	40.0%
IR 500	1.5%	3.0%	26.7%
FDIC 100	1.0%	13.0%	15.4%
Fed 50	0.0%	4.0%	0.0%
Social 50	18.5%	22.0%	63.6%
OTA Members	34.3%	42.2%	11.1%

Figure 9 – DMARC Adoption, 2012-2013

Figure 9 shows the year-to-year growth in adoption of DMARC by senders analyzed in this report. The "Record" column represents the percent of organizations that have a DMARC record, while the "R or Q" column represents the percentage of DMARC adopters that have taken the step of posting a record with a "reject" or "quarantine" directive.

There was growth in all sectors, with OTA members and the Social 50 leading the way in the use of DMARC. The most dramatic growth was seen in the FDIC 100, which increased thirteen-fold from 1% to 13%, driven in part by OTA member companies and the strong support of FS-ISAC and the Financial Services Roundtable. Use of strong policy statements to reject or quarantine also grew, again led by the Social 50, in which 63.6% of DMARC adopters make a strong policy statement. There is obviously room for improvement in all sectors, first to utilize the reporting/feedback feature of DMARC, and then to issue policy directives once the organization is comfortable with the accuracy of their email authentication.

OTA recommends that all senders implement DMARC quickly, at least in "monitor mode" (where no action is specified on mail which fails authentication), to gain experience with the specification and to receive feedback reports to improve authentication deployments. Additional information and resources are available on the OTA website at http://otalliance.org/resources/authentication/index.html.

INBOUND ADOPTION OF EMAIL AUTHENTICATION

While the focus of this report is outbound adoption of email authentication, the full value of email authentication is only realized when both the sender and receiver are participating in the process.

For organizations that send high volumes of email to consumers, it is critical that mailbox providers such as AOL, Comcast, Google, Microsoft and Yahoo! preform inbound email authentication checks to verify the legitimacy of messages. With the rise in spearphishing attacks where criminals pretend to be employees or business partners of an organization, it is critically important that all organizations (both public and private sector) implement email authentication verification on inbound messages to help protect employees and internal systems from attacks.

Because email processing systems vary so widely and sit behind layers of security, it is not possible to track the adoption of email authentication for inbound use. Most email systems can check for DKIM and/or SPF and utilize the results as a factor in determining how to process the messages. To provide businesses, government and other users with maximum protection, DMARC support also needs to be an integral feature in email processing systems. Organizations should contact their email and anti-spam vendors to encourage them to incorporate this support quickly.

OTA strongly recommends that organizations fully utilize any email authentication checking available in their existing systems and look ahead to increased use of inbound checking and DMARC for maximum protection. At a minimum, to address direct spearphishing attacks, organizations should verify authentication on incoming messages purporting to be from their own domains.

DOMAIN LOCKING

New to this year's report, domain locking is important to prevent domain takeovers and points are deducted in the composite analysis if an organization's domain is not locked. Adoption by sector can be seen in Figure 10, and the vast majority of sites adhere to this best practice. Still, this means that 30 of the sites represented in this table (4.2%) need to lock their domains to help protect their brand and users.

2013 Domain & Brand Protection Domain Locking	
IR 100	97%
IR 500	95%
FDIC 100	98%
Social 50	90%
OTA Members	95%

Figure 10 – Domain Locking Adoption

DOMAIN, BRAND & CONSUMER PROTECTION CONCLUSION

Use of email authentication, DMARC and domain locking is critical to protect domains (and associated brands) from abuse and to help protect consumers from spoof messages pretending to be from that brand.

Best practices in this area can be summarized as follows:

- Implement both SPF and DKIM for top-level domains and any major subdomains seen on websites or used for email.
- Implement DMARC for all appropriate domains, initially in "monitor" mode to get receiver feedback and verify accuracy of email authentication, and eventually to assert a ""reject" or "quarantine" policy to receivers.
- Implement inbound email authentication and DMARC support to protect employees and corporate data from spearphishing exploits.
- Ensure that domains are locked to prevent domain takeovers.

As noted in the sections above, overall adoption of email authentication continues to grow, but some sectors lag significantly in use of basic email authentication. There is significant room for improvement in all sectors for support of both SPF and DKIM, as well as for DMARC. While introduced in January 2012, DMARC is still in its infancy but now has the benefit of widespread adoption by consumer ISP's. Domain locking is already practiced by the vast majority of organizations, but should be a required practice and checklist item to ensure proper handling as new domains are created or moved into production.

SITE, SERVER & INFRASTRUCTURE SECURITY

A key aspect of a site's trustworthiness involves the security of the site and infrastructure so that users can be confident data transactions are secure and that they are on the site they expected. In addition to increasing user trust, items in this category also help to protect the site owner's data and systems from attack. Components analyzed in this category include overall sites security and exposure to known vulnerabilities, SSL configuration, use of extended validation (EV) certificates, Always-On SSL (AOSSL), 2048-bit SSL keys, and secure DNS (DNSSEC).

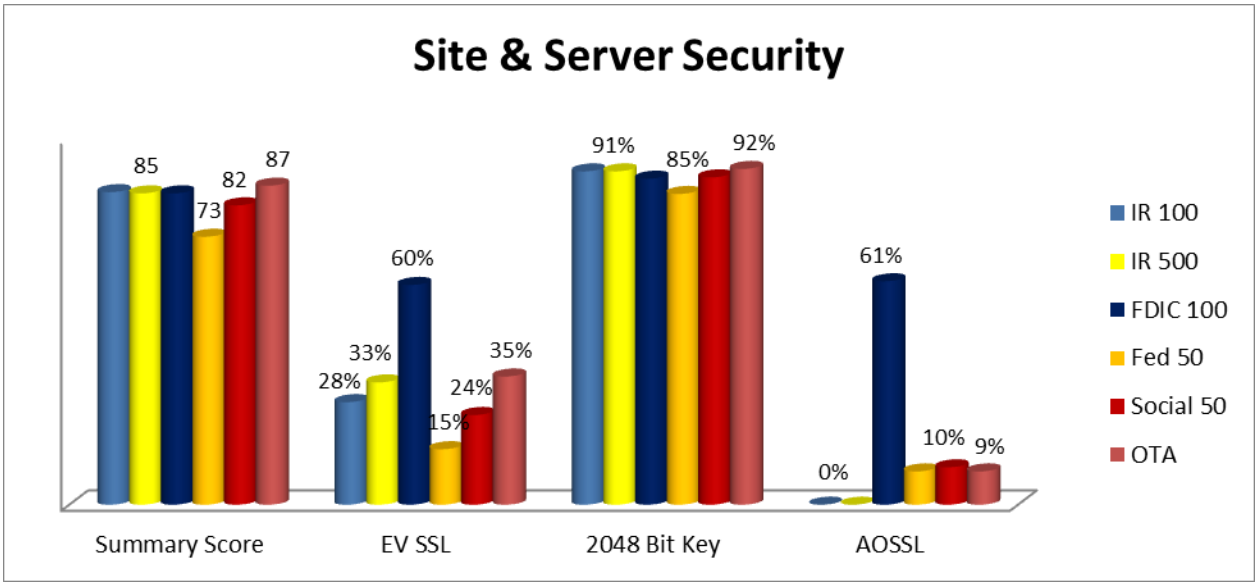

Figure 11 – Site & Server Security Scores/Adoption by Sector

As seen in Figure 11, scores for some components are fairly tight, while others vary widely:

- SSL scores, the core baseline component in this category, are clustered tightly around the overall average of 85, with the Federal 50 the only outlier trailing by approximately 12 points.
- EV SSL adoption, which is awarded bonus points in the composite audit, varies from a low of 15% in the Federal 50 to a high of 60% in the FDIC 100, with most other sectors in the low-middle range.
- Use of 2048-bit SSL keys will become a NIST requirement in January 2014, and was awarded bonus points in this year's analysis. Adoption is already high (~90%) for all sectors, with the Federal 50 slightly lagging at 85%. Sites are encouraged contact their Certificate Authority for upgrades if they do not yet have 2048-bit keys.
- AOSSL helps to ensure that all data interchange with the site and user is secure and helps prevent "sidejacking," where hackers can intercept sensitive information being transmitted via cyber snooping or through misconfigured wireless access points. Adoption ranges from no support in the IR 500 to 61% in the FDIC 100. The Federal 50, Social 50 and OTA members have modest adoption of approximately 10%. Sites who have implemented AOSSL were awarded bonus points.

SSL IMPLEMENTATION ANALYSIS

In reviewing recent forensics and security vulnerability reports from Qualys and High-Tech Bridge, sites' SSL implementation is increasingly being cited as a major source of vulnerabilities and site exploits.[7] Though obtaining and installing an SSL certificate is straightforward, it is often fraught with sever configuration missteps, exposing the site and users to vulnerabilities. According to data from Qualys SSL Labs, in April 2013, only 21.9% of the sites they surveyed were deemed secure, with properly configured servers and protection from known vulnerabilities.[8]

OTA used the Qualys SSL Labs tool (www.ssllabs.com) and High-Tech Bridge Immuniweb service (www.htbridge.com/immuniweb) to evaluate sites' SSL implementation, EV SSL adoption, and use of 2048-bit keys. In early 2013 Qualys upgraded their tool to better evaluate SSL configurations against the current threat environment. The most significant change that administrators will see in their SSL report is a letter grade versus a number score. This report evaluates a site's certificate, use of TLS and SSL protocols and other criteria including key strength, known vulnerabilities such as Beast attack, and PCI compliance.[9]

The 2013 OTA analysis found numerous cases of misconfigured servers. Where possible, OTA made efforts to contact the server administrators to help them protect their site from the visible exploits by sending email to the contact address at the respective domains. In several cases, even large sites were able to confirm the findings and re-configured their servers to reduce their threat potential. While this notification may have impacted some site scores favorably, OTA felt it had the responsibility to contact companies to help improve their site security and protect consumers from potential harm.

2013 Site & Server Security SSL Implementation Scores		
	2012	2013
IR 100	75.9	85.3
IR 500	76.8	85.1
FDIC 100	75.8	85.0
Federal 50	67.7	73.2
Social 50	77.7	82.1
OTA Members	79.8	87.1

Figure 12 – SSL Site Averages

As shown in Figure 12, SSL scores improved in all sectors despite the more rigorous requirements imposed by Qualys SSL Labs. The greatest improvement was seen in the IR 500 and FDIC 100 sectors with nearly 10 point increases.

[7] Source: Qualys 2013 report https://www.trustworthyinternet.org/ssl-pulse/
[8] https://www.trustworthyinternet.org/ssl-pulse/
[9] https://community.qualys.com/blogs/securitylabs/2013/02/07/ssl-labs-update-increases-security-requirements

Site administrators are encouraged to review the SSL Server Rating Guide[10], which provides an overview of the assessment methodology. This resource provides a vendor-neutral tool to assess their SSL server configuration for common configuration issues. The analysis is easily automated and accessible.[11] It is important to recognize that this analysis does not scan for every server attribute or possible combination of vulnerabilities. OTA welcomes feedback to update this tool for ongoing use, and plans to add other site scanning for other vulnerabilities such as cross-site scripting and malvertising exploits in 2014.

EXTENDED VALIDATION SSL CERTIFICATES

Extended Validation SSL Certificates (EV SSL) were introduced in the 2006 report to help address lookalike and phishing sites as well as the issue of fraudulently obtained SSL Certificates. EV SSL requires a thorough verification and audit process that helps prevent deceptive and illicit entities from obtaining a certificate on behalf of a legitimate brand.

EV SSL provides differentiation and recognition for sites by displaying a green identifier as a visual trust indicator in the address bar or browser chrome. EV SSL is supported by all leading browsers including Internet Explorer, Firefox, Chrome, Opera and Safari.

As seen in Figure 13, worldwide use of EV SSL certificates continues to increase, growing more than 28% to exceed 74,000 deployed certificates this year.[12] Growth has been attributed to brands' desire for differentiation, amplified by increased cybercriminal activities and deceptive websites. EV certificate costs are not material, nor do they require changes in infrastructure beyond existing SSL certificates.[13]

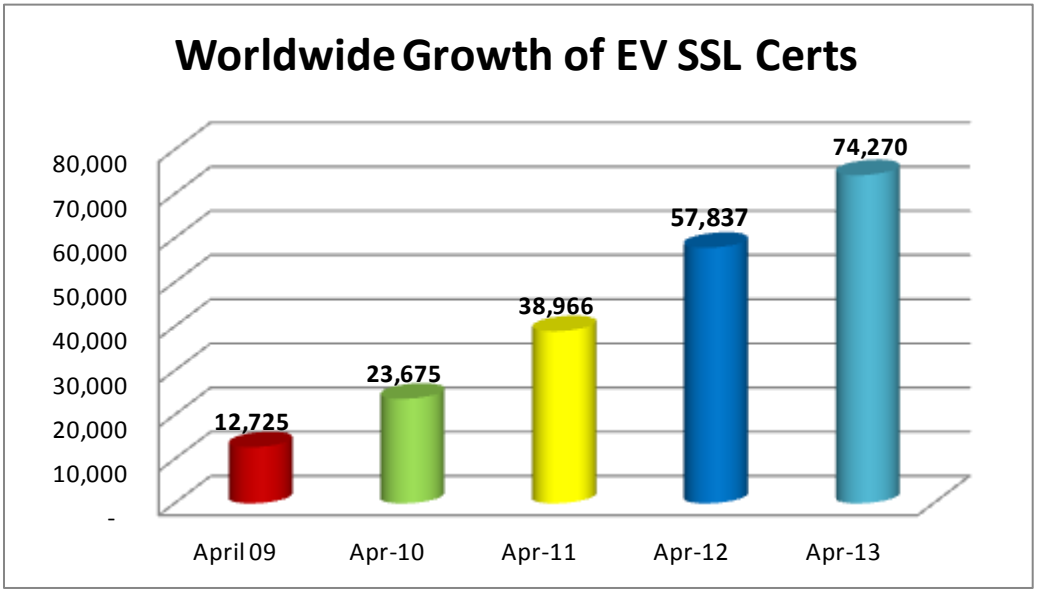

Figure 13 – Worldwide EV SSL Certs, 2009-2013 (Netcraft, 2013)

[10] https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide_2009.pdf
[11] https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.0.pdf
[12] Source: OTA analysis completed April 21 – May 20, 2013 utilizing data from Netcraft published report. http://www.netcraft.com/.
[13] Note the actual number of certificates issued and sold by Certificate Authorities is greater due to the lag in acquisition and deployment.

Figure 14 below shows the year-to-year growth in EV SSL adoption by sector (calculating EV SSL adoption as a percentage of sites with SSL and the larger sectors showed modest but steady growth again this year.

Dips in the Federal 50, Social 50 and OTA members can be attributed to shifts in the lists. The Federal 50 has several new sites on this year's list; the Social 50 was significantly expanded from last year's list of 27 social networks to include leading gaming, blogging, image sharing and dating sites; and OTA membership has expanded to include several companies who are not consumer-facing and historically have not had an incentive to adopt EV SSL. As noted, the FDIC 100 leads adoption (60%) which reflects their efforts to counter the threat of lookalike and phishing sites commonly used to attack financial services and banking customers.

2013 Site & Server Security EV SSL Certificate Adoption				
	2010	2011	2012	2013
IR 100	18.0%	27.3%	27.2%	28.0%
IR 500	26.1%	29.8%	30.7%	33.4%
FDIC 100	25.6%	45.6%	55.0%	60.0%
Federal 50	11.4%	22.2%	25.9%	15.2%
Social 50	-	12.0%	29.6%	24.5%
OTA Members	32.5%	35.3%	43.4%	35.0%

Figure 14 - EV SSL Certificate Adoption by Sector, 2010-2013

DOMAIN NAME SYSTEM SECURITY EXTENSION (DNSSEC)

DNSSEC adds security to the DNS lookup. It is a requirement set forth by the White House as an Office of Management and Budget (OMB) directive issued in August 2008.[14] DNSSEC is designed to help address "Man-in-the-Middle" (MitM) attacks and cache poisoning by authenticating the origin of DNS data and verifying its integrity while moving through the internet. DNSSEC is now deployed in the .com, .gov, .org and .net TLD's, potentially supporting more than 90 million .com domain name registrations worldwide. This is a vital step towards improving the integrity of the Internet.

2013 Site & Server Security DNSSEC Adoption		
	2012	2013
IR 100	0.0%	0.0%
IR 500	0.0%	0.0%
FDIC 100	0.0%	0.0%
Federal 50	70.0%	88.0%
Social 50	0.0%	0.0%
OTA Members	0.0%	7.6%

Figure 15 – DNSSEC Adoption by Sector

[14] August 2009 the Office of Management and Budget (OMB) has told federal chief information officers that they have until January 2009 to deploy Domain Name System Security (DNSSEC) on top level .gov domains. http://gcn.com/articles/2008/08/22/dns-security-steps-ordered-by-omb.aspx

As shown in Figure 17, 2013 adoption of DNSSEC grew in the Federal 50 increasing from 70% to 88%. Netting out Federal Government sites that are .mil or .com government sites the adoption rate increases to 96%. OTA is the only other sector that has sites supporting DNSSEC.

As a result of low market awareness of the technical value and the risk of introducing new points of failure and sources of error associated with DNSSEC, many firms contacted by OTA have elected to delay implementation. Additional contributing factors include lack of support from hosting environments and domain name registrars, lack of integrated browser support and higher priority infrastructure security issues.

SITE, SERVER & INFRASTRUCTURE SECURITY CONCLUSION

To ensure maximum trust and protection of data and systems, sites must implement strong security in their servers and infrastructure. This revolves largely around proper implementation of SSL, which is easy to set up but must be optimized to avoid common vulnerabilities and exploits.

The Qualys SSL Labs tool used by OTA in the core SSL analysis can provide tremendous insight into issues requiring resolution. OTA's experience using this tool with several members and outside companies demonstrates that changes can be made inexpensively and quickly once the issues are identified.

Best practices in this category can be summarized as follows:

- Optimize SSL implementation using information gleaned from tools such as Qualys SSL Labs, with specific focus on vulnerabilities that earn a letter grade of "F".
- Use EV SSL on sites that are frequently spoofed and for sites where users need to be assured they are at a legitimate site.
- Implement AOSSL on sites where a high degree of sensitive data transfer occurs or users are apt to use public wireless access points.
- Use 2048-bit (or higher) SSL keys – this becomes a NIST requirement in January2014.
- Utilize DNSSEC to further protect site's DNS infrastructure from attack and exploits.

As noted in the sections above, average SSL scores have risen in all sectors in the last year. Yet 98 of the sampled SSL sites received an "F" grade, indicating they (and their users) are at risk. EV SSL and AOSSL are strongly supported by the FDIC 100 and enhance trust in the online banking environment. Other sectors are lagging in these areas and need to provide similar protection and assurances for their users.

2048-bit keys are already widely adopted and it is expected that most of the remaining sites will move to the higher-security keys as they renew their SSL certificates. Finally, DNSSEC support is still largely focused in the Federal 50 sector, but is available to all companies who want to harden their security infrastructure.

DATA PROTECTION, PRIVACY & TRANSPARENCY

To engender trust online, organizations must also adhere to strong privacy policies and practices, which imply informed use and consent from users wherever possible. Since 2009, OTA has been advocating for increased transparency and discoverability of privacy policies, including recommending that policies be written for the average site visitor and clear disclosure of data collection, data usage and retention practices as well as any sharing with third parties.

The 2013 report expanded the baseline established in 2012 by looking at honoring of Do Not Track, (DNT) in addition to analysis of privacy policies, site tracking, and public versus private WHOIS registrations. Past data loss incidents and FTC privacy-related settlements or judgments are also factored into the composite score as an indicator of strong data stewardship practices.

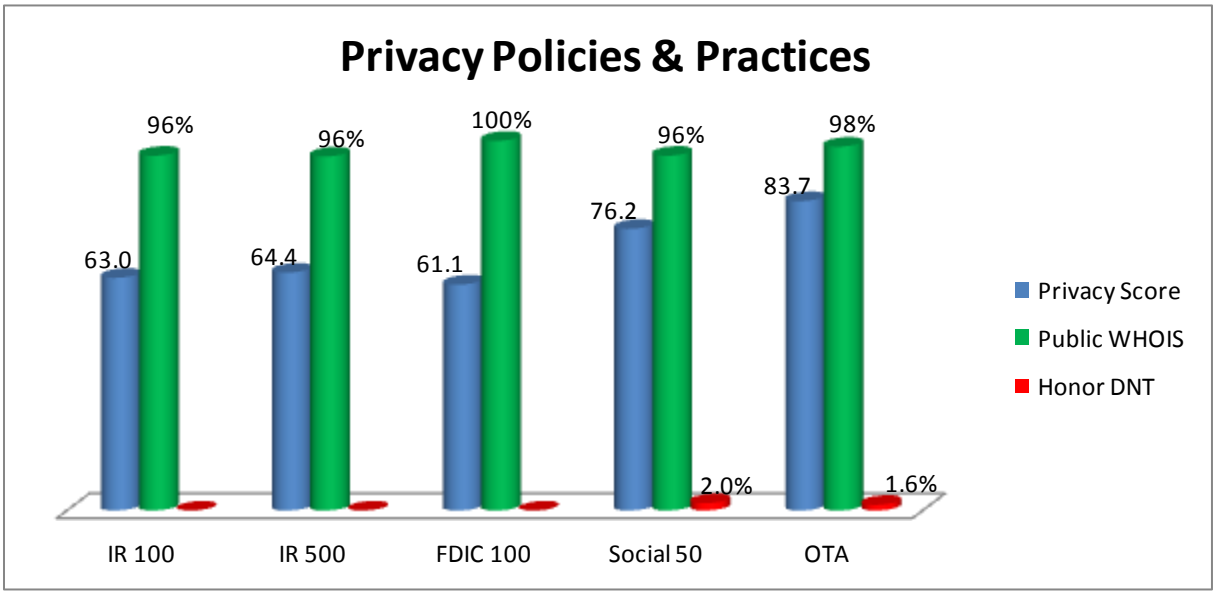

Figure 16 – Privacy Policies and Practices by Sector

Figure 16 shows the average scores and adoption of various components across sectors. The privacy scores for each sector are the core baseline scoring component for this category, with a maximum of 100 points available. Sites with a private WHOIS have points deducted from their total, while those who honor Do Not Track receive bonus points since this is an emerging best practice.

- Privacy scores. Though the overall average score was 66.5, the graph shows two tiers – low 60's for the IR 500 and FDIC 100, and high 70's to mid-80's for the Social 50 and OTA. This is indicative of commerce versus social sites, where commerce sites may be challenged to limit data use, while social networks rely on strong privacy practices in order to be trusted by their users.

- WHOIS registrations are overwhelmingly public, with an overall average of 97% and all sectors at 96% or higher, though this still leaves 23 of the sampled sites (3.2%) with private WHOIS registrations, thus limiting transparency. The vast majority of the private WHOIS registrations are in the IR 500, which has 21 (4.2%) of sites currently set as privacy or by proxy registrations
- Do Not Track (DNT) – While the W3C and industry trade groups are finalizing standards and practices, adoption is in a nascent stage. OTA commends Twitter and others who have supported DNT to provide users increased control over data collection, usage and sharing by third parties.

PRIVACY POLICIES & THIRD PARTY TRACKING

Privacyscore (www.privacyscore.com), a service of AVG Technologies, was the primary tool used to analyze privacy practices for the 2012 and 2013 reports. This tool rates sites on a scale of 100 points, with 50 points possible for evaluation of the site's privacy policy, and 50 points possible based on the privacy qualifications of third-party trackers seen on the site.[15] Augment by OTA staff evaluation of the site's written privacy policy and Privacyscore results, data was tracked for the IR 500, FDIC 100, Social 50 and OTA members. It should be noted that 5 of the Social 50 sites were omitted from this analysis because their privacy policies were not in English and could not be confidently verified. In addition sites may have add-ons or apps which collect and share data that may not have been detected in this analysis.

Though the average scores are acceptable, (overall average of 66.5 and sector averages ranging from 61.1 to 83.7), this is the area in which the highest number of companies received a failing score. Two-hundred thirty seven of the sites (33.7%) had scores below 55. In the FDIC 100, 55 companies had a failing score; followed by the IR 500 (35%). This indicates a bi-modal distribution, with many companies adhering to strong privacy policies and practices while others fall far short.

Clearly there is much room for improvement for many sites. Privacyscore and other related third party tools can provide valuable insight into changes that will improve sites' practices.

DATA BREACH INCIDENTS & FTC SETTLEMENTS

Data breaches and FTC settlements are often indicative of poor data stewardship practices, and have been factored into the composite scoring. Sites with public disclosures receive deductions for any data loss or FTC event reported since April 2011. Such scoring does not automatically exclude one from making the Honor Roll taking into the account many data loss incidents are the result of brute force and FTC settlements are not an admission of guilt.

Data breach incidents occurred in 52 (6.9%) of the sampled organizations. The IR 500 had the lowest rate (2.8%) of breaches, while other sectors were in the 10-15% range. FTC suits or settlements occurred in 8 (1.1%) of the sampled organizations. These were concentrated in the Social 50 (8%) and IR 100 (5%).

[15] Privacyscore methodology http://www.privacyscore.com/faq

DATA PROTECTION, PRIVACY & TRANSPARENCY CONCLUSION

Privacy and data protection are essential to establish trust with online users. By analyzing the privacy policies, third-party tracking, honoring of Do Not Track and recent data breaches or FTC settlements, it is possible to get a comprehensive view of a company's commitment to privacy. As noted previously, though the scores seem reasonable, over one-third of the companies received failing scores, highlighting there is vast room for improvement.

Best practices in this category can be summarized as follows:

- Publish discoverable, easy to find, and comprehendible privacy policies.
- Write policies for the site's target audience and demographics. Consider providing bi-lingual versions representing the diversity of non- English speaking site's visitors. See Spanish version of OTA's privacy policy https://otalliance.org/privacyes.html.
- Create a layered, concise summary linking to an expanded policy. Provide a clear statement including details if, what and for what purposes personal data is being shared with third parties.
- Share details of data retention policies including clarification if such data is retained after the online interaction is terminated. See example https://otalliance.org/privacy_demo2.html.
- Make best efforts to provide notice to consumers if their data is requested by third parties due to legal requirements. Suggested draft copy includes the statement "*To the extent we are legally permitted to do so, we will take reasonable steps to notify you in the event that we are required to provide your personal information to third parties as part of legal process*."[16]
- Only use third-party trackers with strong privacy qualifications and who participate in self-regulatory programs such as NAI.[17]
- Honor sites "Do Not Track" DNT browser settings.

[16] Sites should have a legal review if this draft copy is applicable to their site and business models.

[17] Network Advertising Initiative is a leading self-regulatory association comprised exclusively of third-party digital advertising companies http://www.networkadvertising.org/

CONCLUSION

As the world economy and society at-large become increasingly reliant on the internet, the public and private sectors must increase their commitment to brand, domain and consumer protection; site and infrastructure security; and data protection, privacy and transparency to ensure online trust and the long-term vitality of the internet.

Trust is the foundation of the internet and it is becoming imperative that we move from a compliance mindset to stewardship. While meeting data security and privacy compliance requirements may satisfy the legal and fiduciary responsibilities, it is merely a baseline and may not increase a brand's value proposition.

Ensuring best practices for security and privacy are in place can help minimize account takeovers, shopping cart abandonment and customer churn. While customer service and shipping polices have historically been part of a brands' value proposition, businesses would be well-advised to highlight security and privacy as part of their brand promise.

In the past year, we have seen new levels of sophisticated spearphishing, resilient botnets and malicious advertising compromising nearly every business sector. Compounded by questionable business practices, privacy abuses and sharing of online tracking data, we are at a critical juncture.

At the same time, we are seeing a renewed commitment to stewardship and adoption of best practices. This report, and the accompanying Honor Roll and Online Trust Index (OTI), serve four primary objectives:

- Recognize leadership and commitment to best practices which aid in the protection of online trust and confidence in online services.
- Promote best practices and provide tools and resources to aid companies in enhancing their security, data protection and privacy practices.
- Raise awareness of the risks helping businesses to improve their security and privacy practices.
- Aid consumers in making informed decisions about the security and privacy practices of sites they frequent.

To maximize consumer protection, no single company or constituency can work alone. Only with the collaboration of industry, business, NGOs and government stakeholders can we achieve a "trusted internet" and assure the vitality of online services.

SUMMARY OF RECOMMENDATIONS

OTA is calling on all consumer facing sites and brands to implement the following by November 1, 2013, to enhance consumer protection before the start of the 2013 Holiday season:

1. **Implement both SPF and DKIM** across all domains and subdomains to enhance brand and phishing protection.
2. An issue often overlooked is that many brands have **domains that never send legitimate email**. Site owners need to publish SPF and DMARC records to provide direction to receiving parties to block all such mail purporting to be sent from those domains.
3. **Publish DMARC records** to provide a feedback mechanism to domain holds on their outbound mail streams and to provide prescriptive advice to ISPs and receiving networks.
4. Review **WHOIS information** for accuracy and public disclosure.
5. Review all DNS and domain entries for **domain locking** to help protect from accidental or intentional site redirects/transfers.
6. **Review SSL implementation scores monthly,** specifically addressing top vulnerabilities such as man-in-the-middle attacks, weak protocol suites and BEAST attacks.
7. **Upgrade all certificates** to 2048-bit keys or adopt Elliptic Curve Cryptography (ECC).
8. **Implement Always On SSL** to ensure all data being transmitted is encrypted between the user and site helping to protect against session monitoring / eavesdropping.
9. **Adopt OTA's Top 10 Recommendations** for business, consumer and brand protection https://otalliance.org/news/releases/2012Top10.html
10. **Review all site data collection** and only use third-parties who participate in one or more voluntary self-regulation programs. Review site's privacy policies to ensure data will not be shared inappropriately and audit all third-party tracking and applications added to sites. (See privacy recommendations listed on page 27).
11. Initiate planning and **deployment of DNSSEC**.
12. Make steps to **honor users' Do Not Track (DNT) settings**.

ACKNOWLEDGEMENTS

Data and analysis has been provided in part by: Agari, comScore, DigiCert, GlobalSign, High-Tech Bridge SA, Internet Identity (IID), Mark Monitor, Microsoft, PrivacyChoice, Qualys, Return Path, SiteLock, SSL Labs, Symantec and TrustSphere. Special thanks to OTA members and staff for their strategic input including: Tom Bartel, Joyce Carcaise, Mike Jones, Mike Hammer, Ryan Hurst, Ilia Kolochenko Geoff Noakes, Ivan Ristic, Craig Spiezle, Joe St. Sauver, Liz Shambaugh, Ken Takahashi, Roland Turner, Jeff Wilbur, and Ben Wilson.

ABOUT ONLINE TRUST ALLIANCE (OTA)

The Online Trust Alliance (OTA) is a non-profit with the mission to enhance online trust, while promoting innovation and the vitality of the internet. Our goal is to help educate businesses, policy makers and stakeholders while developing and advancing best practices and tools to enhance the protection of users' security, privacy and identity. OTA supports collaborative public-private partnerships, benchmark reporting, meaningful self-regulation and data stewardship.

As the only global non-profit focused on enhancing online trust with a view of the entire ecosystem, OTA has members across multiple industries, representing the private and public sectors. Members include technology leaders, social networks, e-commerce, financial institutions, service providers, government agencies and industry organizations.

OTA's goals include:

- Enhance Consumer Online Trust and Confidence
- Protect Company Brands and Reputation From Abuse and Cybercrime
- Increase Consumer Choice, Security and Control over Data and Privacy
- Accelerate Adoption of Best Practices and Self-Regulation
- Distinguish Organization Leadership among Industry Peers
- Promote Innovation and the Vitality of the Digital Economy

Revised June 5, 2013
v1