2015 ONLINE TRUST AUDIT and HONOR ROLL

Analysis of the adoption of best practices in:

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

OTA
Online Trust Alliance

Released June 16, 2015
Updated November 17, 2015

TABLE OF CONTENTS

OVERVIEW & BACKGROUND

Now in its seventh year, the OTA Online Trust Audit has become the benchmark audit of businesses' commitment to security, privacy and consumer protection. This report serves as the foundation for business and technical decision makers as they bring new products and services to the market. As the cyber threat increases and privacy concerns heighten, the relevancy and timeliness of this report is significant, underscoring the imperative that data security, protection and privacy need to be integrated into every service, business process, web site and mobile application.

The 2015 Audit reflects input and review through a multi-stakeholder process, evaluating current standards, best practices and leading causes of data breach incidents. A public call for comments was issued in November 2014 in parallel with meetings involving trade organizations, consumer advocates and leaders in the private and public sector. The feedback and recommendations were incorporated into the methodology released in March which includes additional data attributes, enhanced granularity to site security and privacy practices, and increased weighting in several core areas.

By design the Honor Roll recognizes leadership while promoting the critical importance for organizations of all sizes to adopt consumer-centric best practices. Organizations that have embraced these practices and data stewardship are to be commended for their commitment to their customers and stockholders.

For the 2015 report, the authors considered automatically disqualifying an organization if it experienced a data breach. Recognizing there is no perfect security and the desire to not dissuade companies from responsible and timely disclosure of breach and data loss incidents, the 2015 methodology tripled negative scoring associated with a data breach. Therefore, some companies who experienced a breach incident and had top scores in every category were still able to quality for the Honor Roll. This approach strikes the balance between not victimizing the victim, yet raises the bar for the adoption of best practices.

It is important to recognize that this analysis is limited to a slice of time. Based on the dynamic nature of web site and application configurations and the evolving threat landscape, sites' scoring may have changed since the audit was completed. Readers should consider companies who have consistently made the Honor Roll as well as question those that have been conspicuously absent. Businesses that fail to adopt a security and privacy by design culture and a data stewardship mindset risk disenfranchising consumers. Additionally, lack of data stewardship and responsible privacy practices may validate the need for regulatory oversight while increasing the risk of litigation and class-action lawsuits.

All analysis was done anonymously without the participation of the sites being analyzed. Sites were selected based on their ranking within their individual sectors (or membership in OTA). At no time has any organization been able to solicit inclusion or attempt to impact scoring. In instances where a significant vulnerability or risk was identified, OTA abided by responsible disclosure practices and attempted to contact the "at-risk" entity.

SECTORS EVALUATED

The 2015 Audit examined the brand protection, security and privacy protection practices of approximately 1,000 websites across the following sectors:

- 2015 Internet Retailer Top 500 (IR 500)[1]
- FDIC top 100 banks (FDIC 100)
- Top 50 U.S. federal government sites (Federal 50)
- Top 50 social networking and sharing sites (Social 50)
- Top 50 news and media sites (News 50)
- Top 50 Internet of Things providers (IoT 50, top providers of home automation and wearable technologies) – *new in 2015* [2]
- OTA member companies (OTA Members)

With the exception of the IoT 50, all sectors have been evaluated in previous years. While sector definitions and criteria for inclusion have remained constant, individual companies may be added or removed from sector lists due to reported revenues, site traffic ranking and the impact of market consolidation and acquisitions. This consistency allows year-over-year analysis within a sector. For online retailers, the analysis was done for the top 100 retailers ("Internet Retailer Top 100") as well as the full Internet Retailer Top 500, allowing comparison of best practice implementation between larger and smaller companies. The addition of the IoT category provides insight into the rapidly emerging connected device category. For the purposes of this Audit, OTA focused on providers of connected home (home automation) and wearable technologies (health and fitness).

"Twitter is honored to receive the top overall award for the highest score on the OTA Honor Roll. Our consistent top ranking is a testament to the importance Twitter places on user security and privacy. We look forward to working with the OTA to continue raising awareness on security practices that can be used to protect users across the web." – Michael Coates, Trust & Information Security Officer, Twitter

[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, published by Internet Retailer Magazine. For illustrative purposes the 2015 Internet Retailer Top 500 and 2015 Internet Retailer Top 100 are abbreviated "IR 500" and "IR 100" in some charts.

[2] The IoT analysis does not include a review of the respective mobile application and/or local device security, nor necessarily any third party cloud storage the vendor may be utilizing.

METHODOLOGY & SCORING

The criteria used in the Honor Roll are highly relevant to the security and privacy practices companies must implement to maximize online trust and consumer protection. The 2015 Online Trust Audit includes a composite analysis focusing on three major categories:

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

The criteria for this year's report are indicative of the most current best practices supported by industry, standards bodies and government agencies.

Sites were eligible to receive 300 total base points (up to 100 points in each category), and up to 70 total bonus points for implementing emerging best practices. Additionally, organizations could lose up to 65 points for having regulatory settlements, data breaches, observed vulnerabilities and other key deficiencies. The audit criteria are adjusted annually to address the evolving threat environment, responsible privacy practices and the need for all sites to continually monitor their security and privacy practices, thus "raising the bar" for Honor Roll qualification. To qualify for the Honor Roll, sites had to receive a composite score of 80% or better ***and*** a score of at least 55% in each of the three main categories. The minimum scoring requirement was instituted recognizing that sites are built on a "chain of trust" that is only as strong as its weakest link.

"We live in a time when our personal privacy isn't so much eroding away as it is land sliding. Privacy is a fundamental right, and security is inseparably associated with it. I'm proud of our strong and transparent stance on defending privacy and data security. We're thankful for the work the OTA is doing!" – Trevor Zylstra, Chief Operating Officer, SparkFun Electronics

In total, more than 400 million email headers, 1,000 privacy policies and approximately 10,000 web pages were reviewed. Data sampling was completed between April 15 and May 15, 2015. It is important to note that a site's configuration or practices may have changed since the sampling and the data only reflects findings during this snapshot in time. We also recognize that the sites examined might be using other technologies (which our tools or research did not detect) to authenticate domains or subdomains, secure their infrastructures, track users on their sites, etc.

A complete list of criteria, along with notes regarding scoring changes from previous reports, is shown below. The 2015 methodology is posted at https://otalliance.org/initiatives/2015-honor-roll-methodology.

DOMAIN, BRAND & CONSUMER PROTECTION

Best practices to help detect and prevent malicious and spoofed email and protect corporate domains.

- Email Authentication (Sender Policy Framework and DomainKeys Identified Mail) – *part of base score, maximized by implementing both methods at top-level and subdomains*[3]
- Domain-based Message Authentication, Reporting & Conformance (DMARC) – *part of base score (increased weighting for "reject" policy in 2015)* [4]
- Implementation of "opportunistic" Transport Layered Security (TLS) for email[5] – *bonus points (new in 2015)*
- Domain Name System Security Extension (DNSSEC) – *bonus points (increased in 2015)*
- Domain Locking – *penalty if domain not locked*

SITE, SERVER & INFRASTRUCTURE SECURITY

Best practices to secure data in transit and collected by websites and prevent malicious exploits running against clients' devices including desktop, mobile and IoT devices.

- Secure Sockets Layer (SSL) Server Configuration – *part of base score, with increased granularity and requirement levels in 2015, including RC4, SHA1 and Forward Secrecy* [6]
- Evaluation of SSL Certificate type (Domain Validation [DV] or Organization Validation [OV]) – *part of base score (new in 2015)*
- Extended Validation SSL Certificates (EV SSL) – *bonus points (increased in 2015)*
- Always On SSL (AOSSL) – *bonus points (increased in 2015 to reflect security and privacy benefits)*
- Bot detection and mitigation - *part of base score (new in 2015)*
- Web Application Firewall – *bonus points (new in 2015)*
- Testing for XSS, iframe exploits, malware, malicious links – *penalty if these threats exist*

"Microsoft is proud to be named to the Online Trust Honor Roll recognizing our leadership in security and privacy best practices. While there is no perfect security or privacy, this award recognizes companies who have taken a holistic view of consumer protection, user empowerment and data stewardship." – John Scarrow, GM, Microsoft Safety Services

[3] https://otalliance.org/eauth
[4] https://otalliance.org/DMARC
[5] https://otalliance.org/best-practices/transport-layered-security-tls-email
[6] https://ota.ssllabs.com/

DATA PROTECTION, PRIVACY & TRANSPARENCY

Best practices providing users clear notice and control of the data being collected, tracked and shared with third parties.

- Privacy Policy – *50 points of 100 point base score*
- Third Party Tracking on Site – *50 points of 100 point base score*
- Layered Privacy Policy – *bonus points*
- Use of Consumer-Friendly Icons – *bonus points (new in 2015)*
- Localized/Multi-lingual Policy – *bonus points (new in 2015)*
- Do Not Track (DNT) Privacy Policy disclosure – *bonus points*
- Honoring of Do Not Track Browser Settings – *bonus points*
- Implementation of Tag or Privacy Management Systems – *bonus points*
- Public vs. Private WHOIS registration – *penalty if private*
- Data Breach & Loss Incidents – *penalty if incident since January 2014 (increased weight in 2015)*
- FTC / State Legal Settlements – *penalty if settlement since January 2014*

The Audit factors were weighted and scored based on the impact they have on email integrity and risks, consumer protection, website security, consumer transparency and overall best practices that will distinguish an organization and brand from the consumer's 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.

Since the release of the 2015 criteria, several dozen companies including leading banks, retailers and OTA members have contacted OTA asking for guidance. Due to the sensitivity of this data and risk of disclosing vulnerabilities, individual organization's scores and data are not public, nor are they shared with any third party or OTA member. Information will be provided to site owners upon written request and verification. For details, including reporting fees, please email admin@otalliance.org.

"Publishers Clearing House is proud to be named to the OTA Online Trust Honor Roll. We have evolved our data stewardship and privacy practices to enhance consumer protection and meaningful self-regulation, recognizing our success is based on transparency and trust. We are committed to supporting privacy and data security initiatives to protect our members and the online ecosystem." – Sal Tripi, AVP Digital Operations and Compliance, Publishers Clearing House

ONLINE TRUST HONOR ROLL HIGHLIGHTS

The primary goal of the Audit and report is to help drive the adoption of best practices and provide prescriptive tools and resources to aid companies in enhancing their security, data protection and privacy practices. The secondary goal is to recognize companies who have demonstrated a commitment to online trust and consumer protection.

In general OTA has been impressed with the increased engagement of organizations across all sectors that are looking to optimize their scores and understand the methodology. Public support from hundreds of organizations, ranging from consumer-facing sites to technology providers, speaks to the commitment of data stewardship and meaningful self-regulation.[7]

The top overall score was realized by Twitter, who for the third year in a row received the highest score across all sectors. In the Internet Retailer Top 500, American Greetings once again outscored all online retailers and e-commerce sites. These companies have demonstrated a consistent commitment to collaboration and data sharing, including participation in multiple working groups, the standards community and industry associations. The following organizations received the top score in their respective sector:

- Internet Retailer Top 500 – American Greetings Interactive
- FDIC 100 – USAA Federal Savings Bank
- Federal 50 – Federal Deposit Insurance Corporation (FDIC)
- Social 50 – Twitter
- News 50 – Business Week
- IoT 50 – Dropcam

Annually OTA also recognizes the top 10 scoring sites among the Internet Retailer Top 500. This year, due to a tie, 11 companies have been named to the Top 10. Joining American Greetings, the 2015 recipients include Cabela's, Drs. Foster & Smith, Fanatics, GameStop, The Honest Company, JomaShop, Kate Spade New York, Living Social, Netflix and SparkFun Electronics. These companies represent a broad range of retailers, from Netflix (ranked 6th) to SparkFun Electronics (ranked 463rd in the Internet Retailer Top 500). This range confirms that qualifying for the Honor Roll is achievable by companies of all sizes and range of technical resources and skills.

As shown in Figure 1, of the organizations evaluated, 44% qualified for the Honor Roll this year (vs. 30% last year). Both the IoT sector and the Federal 50 were new additions to Honor Roll assessment this year – the IoT as a new sector and the Federal 50 because in prior years the privacy policy base scores were not included in the analysis. The large increase in overall Honor Roll achievement was primarily attributed to the Internet Retailer Top 500, which rose from 24% in 2014 to 42% in 2015. Analysis of this increase

[7] https://otalliance.org/interactive-marketing-security-privacy-communities-embrace-ota-audit-honor-roll

revealed that nearly 100 e-commerce companies who in earlier years had been close to qualifying made simple, straightforward improvements in their site security and privacy practices.

Overall, fewer companies repeated this year than last, highlighting that security and privacy practices are not a static process – sites need to continually monitor, update and evolve to keep pace with evolving threats. A complete list of Honor Roll recipients by sector can be found in Appendix A. Approximately one-sixth of qualifiers (68) achieved Honor Roll status for the fourth year in a row, nearly one-seventh (56) qualified for the third year in a row, only one-eighth (45) qualified for the second year in a row, and more than half (212, mainly from the retail sector) were first-time qualifiers.

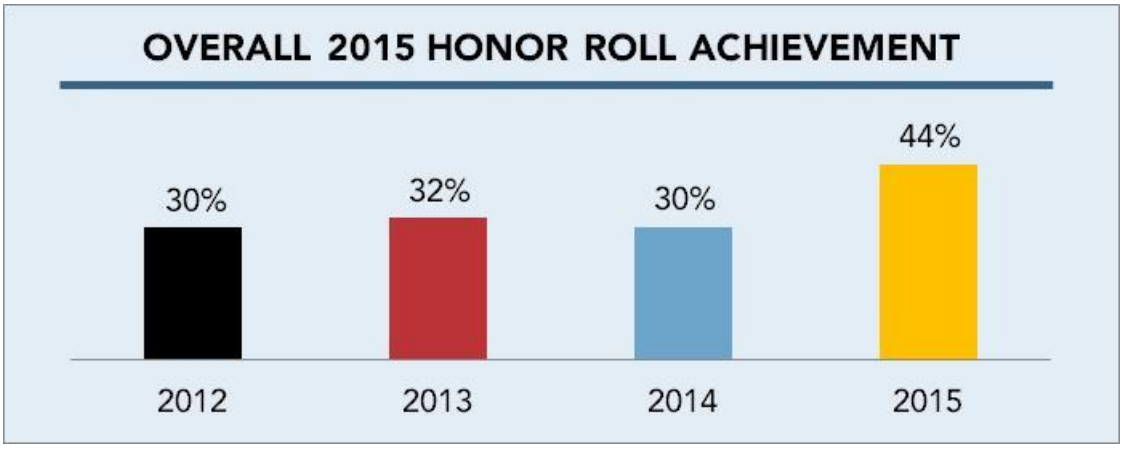

Figure 1 – Overall Honor Roll Achievement by Year

As illustrated in Figure 2, Honor Roll achievement grew in all sectors despite more stringent criteria in this year's Audit. As in the past two years, the Social 50 outscored all sectors with 58% achievement. Follow-up discussions with honorees in this sector revealed that a major factor in their high scores was homogeneous and integrated system architectures, in contrast to other sectors which have a higher percentage of legacy systems. Online retailers, banks and federal government sites all achieved results in the 40% range, while the IoT 50 and News 50 lagged with 20% and 8% achievement respectively.

"We are honored to be recognized in the Online Trust Honor Roll. This follows our commitment to the security, privacy and consumer protection of our customers. We believe data stewardship needs to be integrated into every service and business process. We are proud to be a leader and a trusted multi-channel retailer." – Richard Armour, Senior Director of Multichannel Operations, GameStop, Inc.

It should be noted that OTA Members, 97% of which qualified for the Honor Roll, have been omitted from the chart since their scores distort and compress the axis. While this achievement is significant, the result may be biased since companies who are members of OTA by the nature of their OTA membership are committed to data stewardship and responsible privacy practices. It should also be noted that the high

achievement of OTA members somewhat skews the overall Honor Roll achievement shown in Figure 1 – if OTA members were excluded, overall achievement this year would drop 4% to 40%.

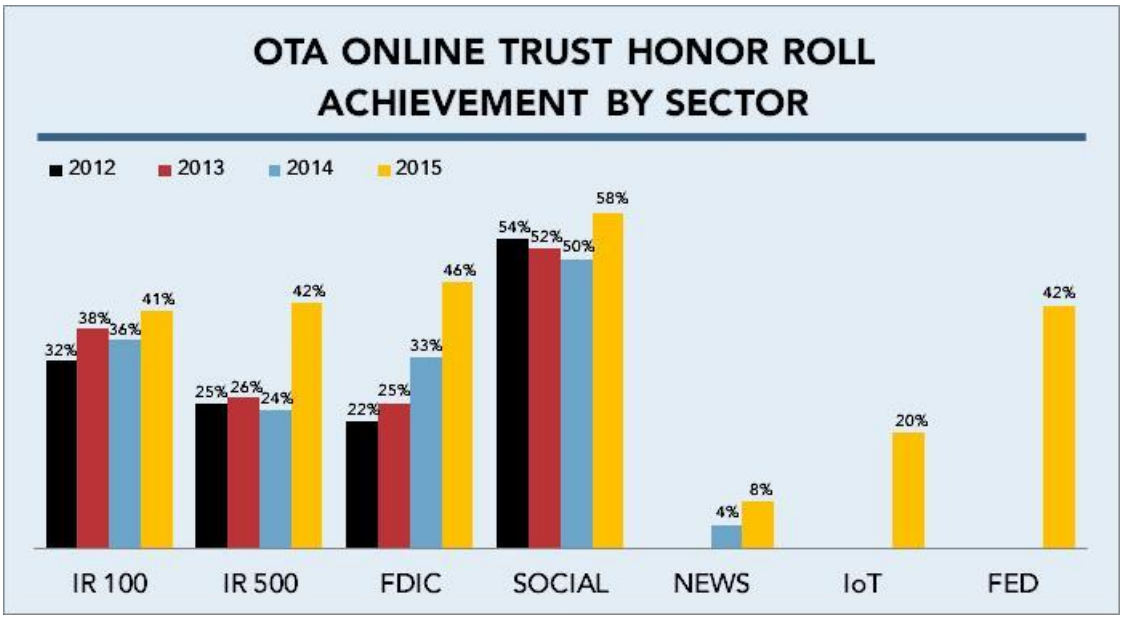

Figure 2 – Percent Achieving 2015 Honor Roll Status by Sector

Reviewing year-over-year trends, growth was noted in all sectors, with a dramatic rise for the Internet Retailer Top 500. There was no single practice which drove the increase – most sectors were flat to slightly up in their baseline scores in the three main categories, though the most consistent increase was seen in baseline privacy scores due to increased transparency of data practices. A record number of companies and organizations achieved the Honor Roll for the first time. As noted previously with the e-commerce sites, many sites were just below the threshold in prior years and qualified for the 2015 Honor Roll by implementing a few additional key best practices. Based on increased concerns regarding government monitoring of the Internet and associated privacy issues, privacy policies for the Federal 50 were evaluated for the first time this year, allowing a direct comparison to all other sectors.

It is also useful to examine the reasons why organizations did not achieve Honor Roll status. Of all sites analyzed, 46% had a failing grade (<55%) in one or more categories, highlighting significant concerns regarding data security and privacy practices. Figure 3 shows the percentage of each sector that had a failing grade, while Figure 4 breaks that down a step further to show which categories caused the failures.

Failures were most prominent in the News 50 and IoT 50 sectors, and least prominent in the Social 50 (the failure rate for OTA members, which is not shown, was 3%). Considering the sensitivity of the data collected by the IoT segment, the failure rate is a wakeup call for the need for guidelines and potential regulatory oversight.[8] The Internet Retailer Top 100 fared slightly better than the Internet Retailer Top 500, as they have the past three years. The Federal 50 had a higher than average failure rate, though 42%

[8] See recommendations from the IoT trustworthy working group https://otalliance.org/IoT

of the sector made the Honor Roll, yielding a bi-modal distribution where organizations either made the Honor Roll or failed in one or more categories (only 4% were neither).

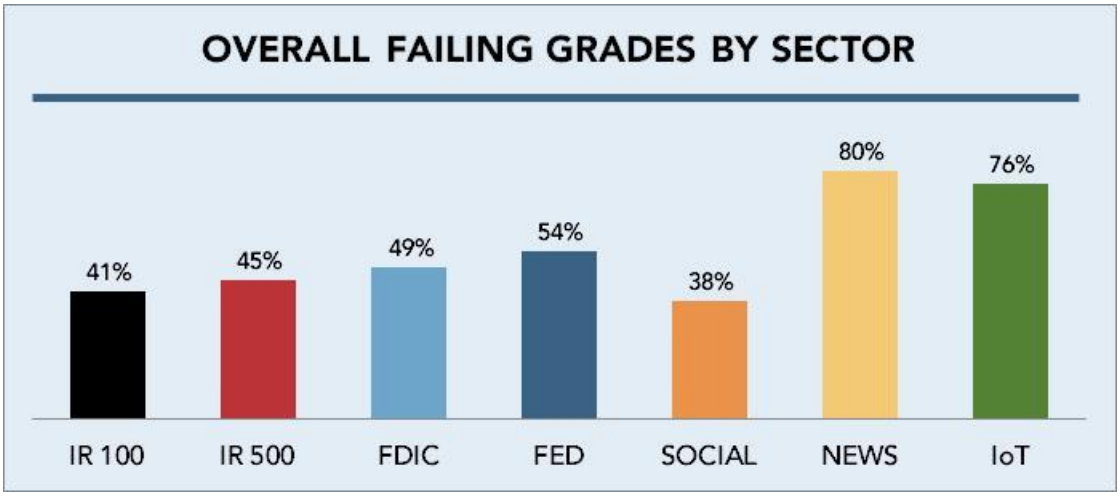

Figure 3 – Percent of Organizations with Failing Grade by Sector

Inadequate domain, brand and consumer protection was the primary cause for failures in the FDIC 100, Federal 50 and IoT 50. The main reason was a continued shift in scoring to place increased emphasis on comprehensive implementation of email authentication and associated DMARC records. This was especially damaging to the IoT 50, which had inadequate email authentication practices. The absence of such practices leaves consumers increasingly vulnerable to spearphishing and related exploits including ransomware, bank account take-overs and identity theft.

"Hayneedle's inclusion in the OTA Online Honor Roll testifies to our commitment in making the online shopping experience for home furnishings and décor safe and secure for our customers. We look forward to our partnership with OTA in preserving our customers' trust and confidence in shopping with us for everything home." – Ryan Paulson, VP of Technology, Hayneedle

Inaccurate and inadequate privacy policies and practices were the next largest cause of failures, impacting half of the News 50, one-third of the top 100 retailers, and one-fourth of both the top 500 retailers and the IoT 50. The News 50 sector had the lowest scores across all sectors for both privacy policies and third-party site tracking, reflecting their reliance on third-party advertisers to drive revenue. The FDIC 100 showed the biggest improvement, reducing privacy failures from 34% last year to 15% this year through enhanced disclosures within their published privacy policies and reduced data sharing with third parties. This is the second year in a row that the FDIC 100 demonstrated major improvements in privacy. Site security was the lowest cause of failure for all sectors, showing that the vast majority of organizations are tracking with the minimum recommendations for site security.

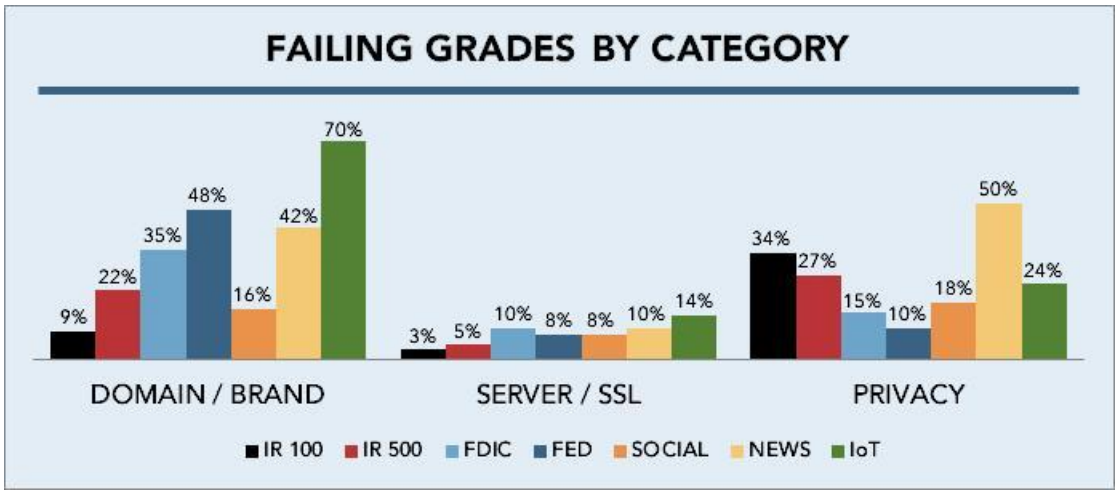

Figure 4 – Percent of Companies with Failing Grade by Sector and Category

The Online Trust Index (OTI), introduced in 2012 and shown in Figure 5 for a year-to-year comparison, provides a normalized view of scoring among sectors. The OTI is calculated as an average composite score across all methodology categories, using a normalized score of 1 to 100. Despite 2015's more rigid criteria, just as in Honor Roll achievement, improvement was seen in all sectors. The News 50 and IoT 50 noticeably lag other sectors, which is not surprising given their low Honor Roll achievement and high failure rates in multiple categories. Again, the poor performance by the IoT category and the risks associated with connected devices underscore the need for increased focus on security and privacy in this sector.[9]

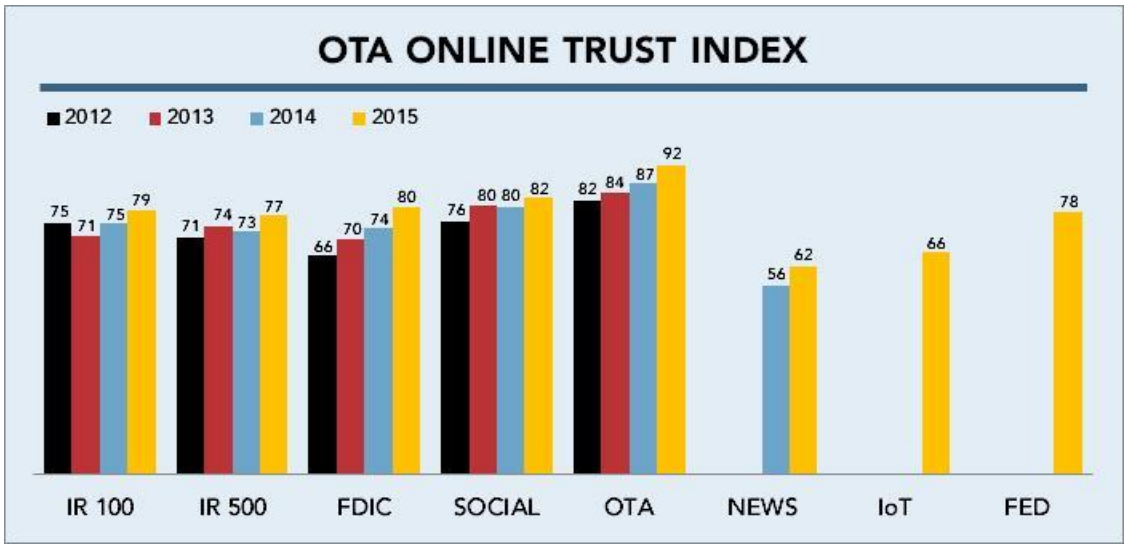

Figure 5 - Online Trust Index by Sector

[9] OTA is proposing a framework to address key security, privacy and sustainability issues (associated lifecycle risks).

Figure 6 provides insight into the performance of each sector, including the high and low normalized scores along with the median score for each sector. Online retailers and the IoT 50 have the highest variation while OTA members have the smallest. Note that some maximum scores exceeded 100 due to qualifying for bonus points. This chart illustrates how the median for several sectors (online retailers, FDIC 100, Federal 50 and Social 50) sits at the 80% threshold, and through some simple operational changes and support of best practices many more organizations were able to qualify for the Honor Roll.

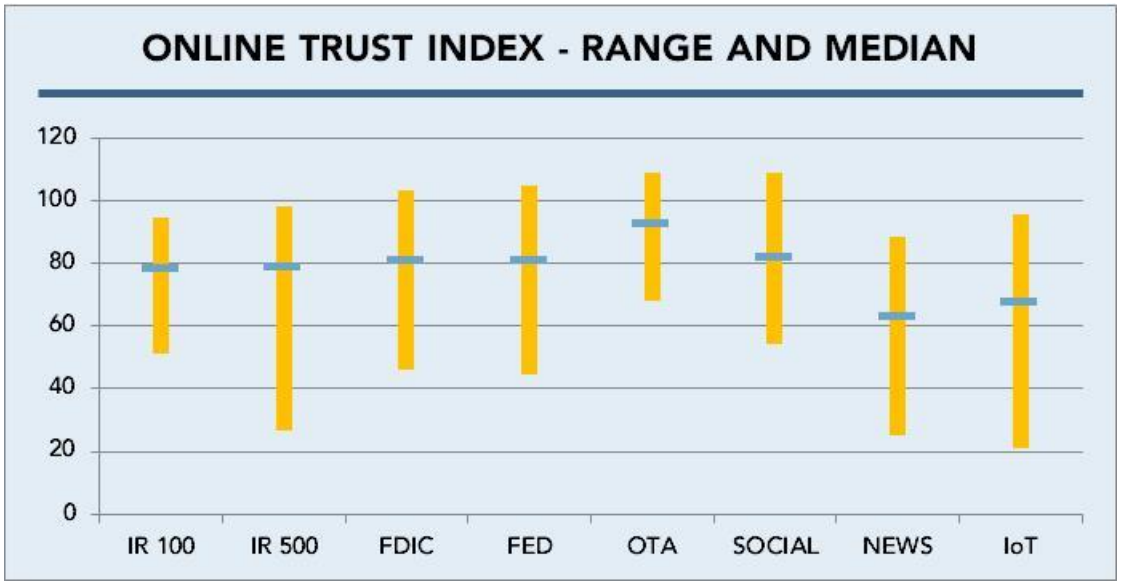

Figure 6 – Range and Median Online Trust Index Scores by Sector

Figure 7 shows the baseline scoring breakdown (out of 100) for all sectors by major category. This chart shows much more variability than the overall OTI scores, especially in the Domain/Brand and Privacy categories. Site security scores are more tightly clustered.

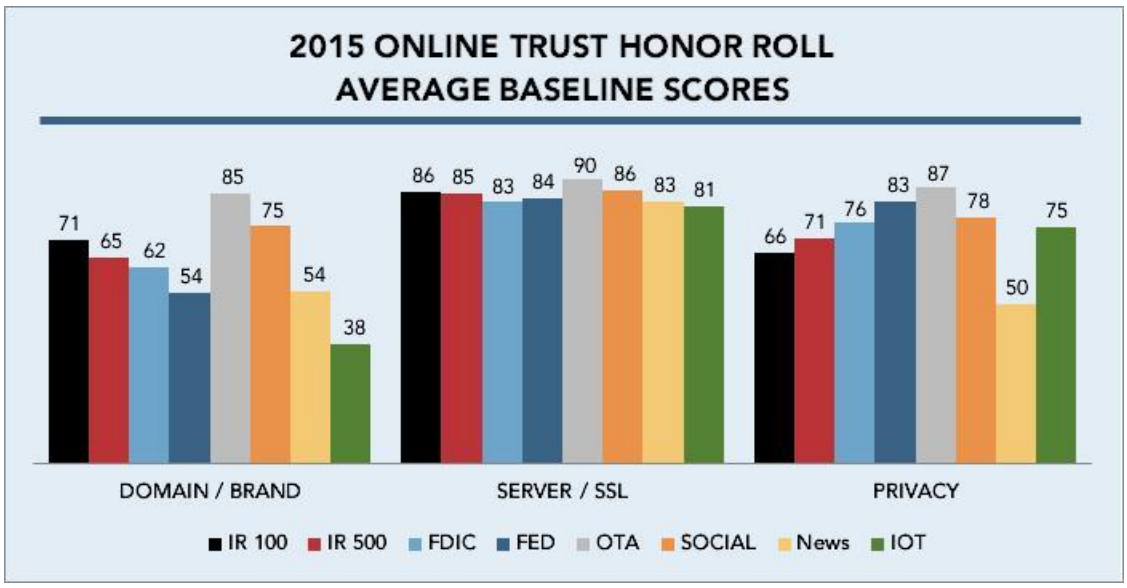

Figure 7 – Major Category Scores by Sector

The primary driver of Domain/Brand scores is the implementation of email authentication on top-level and subdomains. As observed in previous years, low scores are primarily due to lack of support for SPF and DKIM at the top-level domains. This continues to be a concern since most spoofing and malicious email purports to come from the most recognizable corporate domains rather than marketing subdomains which are often delegated to email-service providers. While email marketers have embraced email authentication primarily to drive deliverability and inbox placement, increased focus and engagement is needed at the corporate level to help maximize brand and consumer protection.

"We're honored to be selected again to the OTA Honor Roll and look forward to continuing this trend. We value security, privacy and trust as the basis on which to build consumer relationships. We continue to share and promote the OTA directions in these areas." – Joseph Yanoska, Executive Director, American Greetings Interactive

Building on these email authentication protocols, DMARC provides ISPs and corporate networks direction on how to handle email that fails authentication. Implementation of DMARC requires only the simple addition of a text record to the DNS file. Adoption has no cost and no impact to server performance, yet the low rate of adoption is concerning and may be indicative of low awareness of the criticality and business value.

Privacy scores improved in all sectors compared to 2014, though there is still wide variation between sectors. Low scores are due to lack of clear notice in privacy policies, incomplete and outdated privacy policies, and use of website trackers that share information with other entities. Improving these scores is generally straightforward via simple updates to the site's privacy policy and a re-evaluation of data sharing practices, including those of a site's service provider(s). This is the first year the Federal 50 has been evaluated in the privacy area, and they had the highest score other than OTA members, primarily since they do not support advertising or share any data with third parties.

"At Netflix, maintaining the trust of our 62 million global members is paramount. Critical to our success is our commitment to protecting the privacy and security of consumer personal data. We applaud OTA's efforts in advancing best practices to enhance online trust, and are honored to have been named to the Online Trust Honor Roll." – Lara Kehoe Hoffman, Global Director, Data Privacy and Security, Netflix

INDIVIDUAL BEST PRACTICES HIGHLIGHTS

DOMAIN, BRAND & CONSUMER PROTECTION

- Email Authentication (SPF & DKIM) – Adoption has reached nearly 100% in several sectors, and lagging sectors have shown growth. Growth is especially strong in use of both SPF and DKIM (FDIC 100 adoption rose from 49% to 63%, and the Federal 50 more than doubled from 22% to 48%). The newly evaluated IoT 50 lags significantly in adoption of basic email authentication – this is likely due to new market entries and traditional companies introducing connected devices without considering security and privacy by design approaches.

- Domain-based Message Authentication, Reporting & Conformance (DMARC) – Adoption continues to rise in all sectors, but is disappointingly low overall (all but OTA and the Social 50 are less than 25%) considering the ease of implementation and proven technical and brand protection benefits. For organizations with a DMARC record, use of "reject" or "quarantine" policies is growing modestly but is also low (only the Social 50 is higher than 25%).

- Opportunistic Transport Layered Security (TLS) – This element, new in 2015, has an adoption rate ranging from 14% (Internet Retailer Top 500 and News 50) to 52% (OTA members). With increased concern about monitoring of email in transit between servers, adoption is expected to rise and may shift from bonus points to baseline scoring in 2016.

SITE, SERVER & INFRASTRUCTURE SECURITY

- SSL Server Configuration – Despite additional and more rigid criteria, scores stayed flat or slightly increased in all but the FDIC 100, which had a modest dip.
- Extended Validation SSL Certificates (EV SSL) – Worldwide use grew more than 19% to nearly 124,000 deployed certificates. Adoption is led by the FDIC 100 (67%) with most other sectors in the 20%-30% range.
- Always On SSL (AOSSL) – While the FDIC 100 leads all sectors with 78% adoption, other sectors are recognizing the benefit of encrypting entire user sessions to optimize security and privacy – most increased adoption 15%-20% compared to 2014. Because this standard is now being promoted by Google and several browsers, sites that do not support it will see reduced search engine optimization (SEO) as well as browser warnings, which could impact site click-through and shopping cart abandonment. Shifting from bonus to base scoring is under consideration for 2016.
- Web Application Firewall – Introduced in 2015, adoption of this practice averaged 35% across sampled sites, led by the Internet Retailer Top 100 (47%) and Federal 50 (46%). Social sites lagged at 12%. Shifting to baseline scoring for 2016 is under review due to the vulnerability and resulting attack vector for sites without firewalls.
- Domain Name System Security Extension (DNSSEC) – Only the Federal 50 has significant adoption (90%). No other sectors have more than 5% adoption. DNSSEC continues to struggle as an IT priority in spite of its technical value.

DATA PROTECTION, PRIVACY & TRANSPARENCY

- Privacy Policy & Third Party Tracking – Scores rose in all sectors this year, most significantly in the FDIC 100 (from 60 to 76) and the Internet Retailer Top 500 (from 64 to 71). The News 50 still lags significantly with a score of 50. The newly evaluated Federal 50 scores strongly (83) with the highest non-OTA Member score across all sectors.
- Layered Notice – Adoption of this practice nearly doubled (21% of sampled sites *vs.* 11%) since its introduction last year. Leading sectors were the Internet Retailer Top 100 (43%) and the News 50 (38%). The new IoT 50 lagged at only 10%. This is an emerging best practice that is gaining momentum and is expected to be incorporated into base scoring in future audits.
- Use of Icons – New in 2015, only 1% of overall sampled sites (all in the online retail and social sectors) have adopted this practice which helps consumers navigate privacy policies more easily.
- Multi-Lingual Policies – New in 2015, 4% of sampled sites follow this practice, with a few adopters in each sector.
- Do Not Track (DNT) Disclosure – Introduced in 2014, this tracks whether the privacy policy specifies support of DNT on the site. Adoption has grown significantly, with 23% of sites providing such disclosure (vs. 13% last year), led by the Internet Retailer Top 100 (52%). Other sectors nearly doubled to the 25%-35% range, while the Social 50 lags at 14%.
- Honoring of Do Not Track (DNT) Browser Settings – This practice has very low adoption, supported by only 11 sites across all sectors. Since the W3C standard is now complete, adoption is expected to increase.
- Support of Tag Management/Privacy Solution – Introduced in 2014, this metric tracks whether a site utilizes a tag management system or privacy solution, and was added to recognize sites that are addressing the complexity and difficulty of managing third-party data collection. Overall, 55% of sites have adopted such a solution (*vs.* 42% last year), indicating it has become an established best practice and as such may be integrated into baseline scoring in future audits. The Internet Retailer Top 100 leads adoption with 84%, followed by the News 50 (74%). Not surprisingly, the Federal 50 lags adoption at 22% since they do not rely on advertising and therefore have little need for such solutions.
- Data Breach & Loss Incidents – Despite many high-profile breaches last year, the number of breaches in sampled organizations dropped from 58 in the 2014 report to 32 this year. The FDIC 100 had the highest rate (9%) followed by the Social 50 (8%). The News 50 was the lowest (2%). Though it is recognized there is no perfect security and that breaches and data loss incidents can happen in any organization, the penalty for a breach was tripled this year due to its impact on consumer trust.
- FTC / State Settlements – Only five of the sampled organizations (all in the Internet Retailer Top 500) had FTC/State suits or settlements since January 2014.

SECTOR HIGHLIGHTS

INTERNET RETAILER TOP 500

- A dramatic increase in Honor Roll achievement (24% to 42%) was observed, primarily due to many companies who in 2014 were just under the threshold making straightforward improvements to increase their score 10-15 points, thereby qualifying them for the 2015 Honor Roll.
- Rallied to address mounting privacy concerns, increasing the average privacy score from 64 to 71 by addressing core privacy policy issues. Top non-OTA sector in supporting both SPF and DKIM (78%) and near top in implementing a tag management/privacy solution (62%).

FDIC 100

- Significant growth in Honor Roll achievement (33% to 46%), mainly due to improved privacy scores. Far outpaces all sectors in EV SSL adoption (67%) and AOSSL adoption (78%).
- Strong growth in adoption of both SPF and DKIM (49% to 63%), yet one-third of banks still failed in this area. Significant improvement in average privacy policy score (60 to 76), reducing failures in this area from 34% to 15%.

SOCIAL 50

- Scored as the top non-OTA sector for percentage of companies making the Honor Roll (58%), as well as having the highest average Domain/Brand, Server/SSL and Privacy baseline scores.
- Top sector for DMARC adoption (48%) and strong second to FDIC in AOSSL adoption (35%).

FEDERAL 50

- Strong showing for initial Honor Roll evaluation with 42% achievement. Realized the highest average privacy score (83) other than OTA member companies. Significant improvement in Server/SSL score (84 *vs.* 71 last year). Primary adopter of DNSSEC (92%, the next highest sector is 5%).
- High sector failure rate (54%), leaving only 4% that neither failed nor made Honor Roll. Though support of both SPF and DKIM more than doubled (22% to 48%), primary failure reason was poor email authentication (lags all but IoT 50), especially support of DKIM at the top-level domain.

NEWS 50

- Lowest Honor Roll achievement (8% *vs.* overall average of 44%), driven mainly by highest overall sector failure rate (80%). Failures were due to poor email authentication (failing scores for 42% of the sector) and failing privacy scores (50% of the sector).
- Though overall privacy scores were lower than any sector (50 out of 100), they had highest the adoption of multi-lingual privacy policies (10%) and highest adoption of tag management/privacy solutions (74%) and layered privacy notice (38%) outside of the Internet Retailer Top 100. As noted in the 2014 report, many sites (26%) have no SSL support though they have logins and collect user profiles, meaning private information is being transmitted "in the clear".

INTERNET OF THINGS (IoT) 50 (new in 2015)

- Overall, solid privacy scores (75) and adoption of privacy practices (60% have a tag management system/privacy solution, 30% include a Do Not Track disclosure), but 14% do not have a discoverable privacy policy.
- Second-highest sector failure rate (76%), almost entirely due to poor email authentication support (70% of the sector failed the Domain/Brand category, where the average baseline score was 38, 16 points below next highest sector). Lowest adoption of any sector for key measures of "SPF or DKIM" (62%), "SPF and DKIM" (30%) and DMARC (2%) – trails next highest sector by nearly 20% in all three measures. This gap is attributed to the prevalence of small startup companies as well as mature companies making their first entry into data collection. Since devices provided by these companies collect and process the most sensitive and personal data of all categories, OTA believes consumer trust and data stewardship will be key success factors and points of differentiation (see OTA IoT Trustworthy Working Group[10]).

"We're honored to be named to the Honor Roll as we continue our commitment to privacy best practices. As more devices become connected in the IoT era, companies must proactively take steps to help protect consumers and be transparent in how this vast amount of data is collected and used." – Chris Babel, CEO, TRUSTe

[10] IoTWG https://otalliance.org/IoT

DOMAIN, BRAND & CONSUMER PROTECTION

By utilizing email authentication (SPF and DKIM), organizations can help protect their brands and prevent consumers from receiving spoofed and forged email. Email authentication allows senders to specify who is authorized to send email on their behalf. Building on email authentication protocols, DMARC adds a policy assertion providing receivers direction on how to handle messages that fail authentication. TLS provides a means to encrypt messages between mail servers, protecting both the brand and consumer. Domain locking ensures that domain ownership cannot be transferred without the owner's permission, further helping to protect a site's brand from abuse. Domain Name System Security Extension (DNSSEC) adds security and integrity to the DNS lookup, helping to prevent "Man-in-the-Middle" (MitM) attacks, cache poisoning and related DNS attacks.

"The OTA Online Trust Audit Honor Roll highlights best practices in security, privacy and consumer protection which every company should strive for. We believe in walking the talk and are honored to be recognized for our commitment to consumer protection. We encourage all our customers to do the same." – Michael Brown, President and CEO, Symantec

An accompanying report will be issued later this year providing in-depth review of email authentication practices and adoption. This planned report will include a deep dive of DMARC, including an analysis of the adoption of reject or quarantine policies. These DMARC policy assertions are recommended best practices to maximize brand and consumer protection by providing receiving networks and ISPs direction to reject messages which fail email authentication verification.

Best practices include:

- Implement both SPF and DKIM for top-level domains, "parked" domains (not used for email) 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.
- Implement opportunistic TLS to protect email in transit between mail servers.
- Ensure that domains are locked to prevent domain takeovers.
- Implement DNSSEC to further protect a site's DNS infrastructure from attack and exploits, including man-in-the middle exploits.

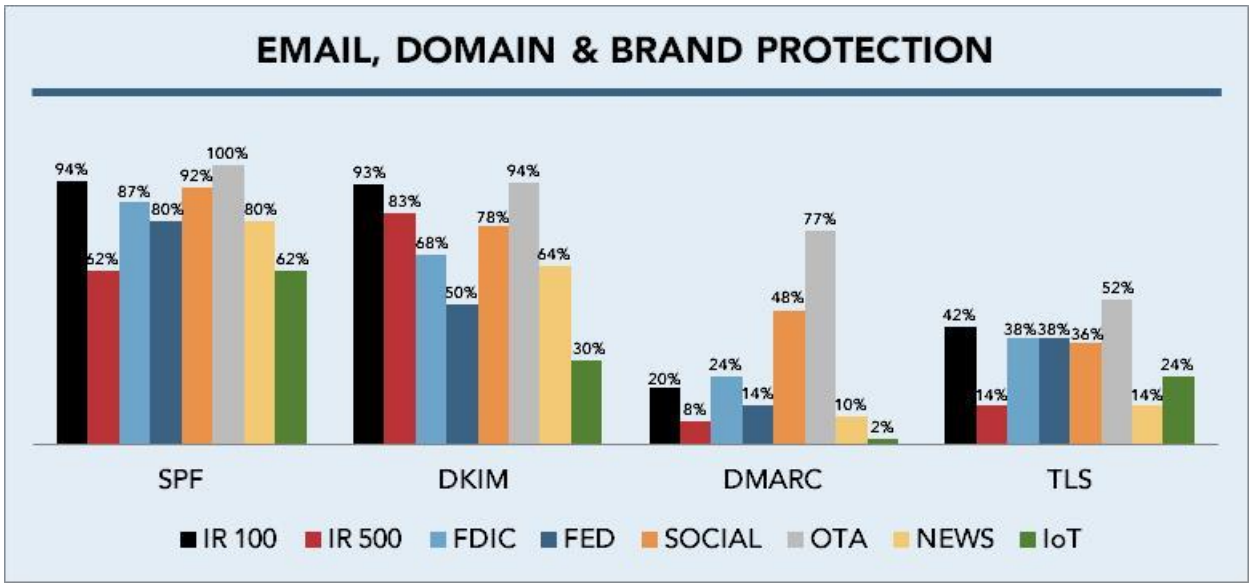

Figure 8 – Email Authentication, DMARC, TLS Adoption by Sector

EMAIL AUTHENTICATION

Analysis of organizations' email authentication support was conducted by OTA and utilized data from Agari, Microsoft and Return Path. Email authentication technologies, namely Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM), help prevent phishing and spam. OTA has tracked the progress of email authentication technologies, best practices and adoption since 2005 and continues to communicate their value to enhance brand and consumer protection and offer training and resources.

As shown in the summary chart in Figure 8, email authentication adoption varies widely across sectors, led by online retailers, social networks and OTA members, while federal government sites and the new IoT sector lag considerably. Lack of authentication impedes receiving networks and ISPs from accurately detecting and blocking malicious and fraudulent email purporting to come from an organization, putting both the recipient and the purported sender's trustworthiness at risk. In general SPF adoption is higher than DKIM adoption across all sectors, primarily due to its ease of implementation, whereas DKIM requires additional configuration and updates to outbound mail servers. Adoption of DMARC continues to rise, with OTA and social sites leading the way.

Organizations worldwide have found that adoption of both SPF and DKIM best enables receivers to detect and block forged and malicious email, while reducing the risk of false positives from mail being forwarded or sent from mailing lists.

As seen in Figure 9, use of both SPF and DKIM grew in all sectors, most dramatically in the Federal 50 and FDIC 100, and online retailers have overtaken social sites as the leading non-OTA sector. It is evident that online retailers and social platforms, which are most heavily reliant on email interaction with their users/customers, have recognized the brand value of email authentication. Though encouraging, much of the growth has occurred via implementation of DKIM at marketing or purpose-specific subdomains – further effort is needed to protect top-level and corporate domains from abuse.

DOMAIN & BRAND PROTECTION BOTH SPF AND DKIM				
	2012	2013	2014	2015
Internet Retailer Top 100	56%	76%	88%	90%
Internet Retailer Top 500	43%	56%	74%	78%
FDIC 100	34%	49%	49%	63%
Federal 50	10%	20%	22%	48%
Social 50	63%	72%	74%	76%
OTA Members	59%	69%	83%	94%
News 50	-	-	50%	56%
IoT 50	-	-	-	30%

Figure 9 – Adoption of Both SPF and DKIM by Sector

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

Introduced in early 2012, 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 became a baseline scoring component in 2013 and received increased weighting for the 2014 report. In 2015 weighting was again increased for use of DMARC reject and quarantine policies, with maximum points awarded to organizations that publish a reject policy.

DMARC ADOPTION					
	2012	2013	2014	2015	
	Record	Record	Record	Record	R or Q
Internet Retailer Top 100	2.0%	5.0%	15.0%	20.0%	15.0%
Internet Retailer Top 500	1.5%	3.0%	6.2%	8.2%	22.0%
FDIC 100	1.0%	13.0%	21.0%	24.0%	20.8%
Federal 50	0.0%	4.0%	6.0%	14.0%	14.3%
Social 50	18.5%	22.0%	36.0%	48.0%	58.3%
OTA Members	34.3%	43.8%	59.4%	76.6%	12.2%
News 50	-	-	10.0%	10.0%	20.0%
IoT 50	-	-	-	2.0%	0.0%

Figure 10 – DMARC Adoption by Sector

Figure 10 shows the year-to-year growth in adoption of DMARC. Use of DMARC records grew in all sectors, and some (Federal 50, Social 50, OTA members) made large leaps. Given the gap between SPF/DKIM adoption (above 90% in many sectors) and DMARC adoption (below 25% in most sectors), there is still significant room for growth in DMARC adoption. The "R or Q" column shows percentage of organizations with a DMARC record publish a reject or quarantine policy, illustrating significant room for growth in nearly all sectors.

INBOUND ADOPTION OF EMAIL AUTHENTICATION

With the rise in spearphishing and associated attempts to compromise business users' passwords and system access, it is critically important that all organizations – in both public and private sectors – implement email authentication verification on inbound messages to help protect employees and internal systems from attacks.

While the focus of this Audit has been organizations' outbound adoption of email authentication for brand and consumer protection, the full value is only realized when both the sender and receiver are participating in the process. While consumer mailboxes have overwhelmingly adopted inbound authentication, corporate and governmental agency adoption remains a serious concern.

OPPORTUNISTIC TRANSPORT LAYERED SECURITY (TLS) FOR EMAIL

Tracking of Opportunistic TLS has been added this year to help address the privacy concerns prompted by both criminals and government actions. TLS effectively encrypts messages in transit from one server to another and de-encrypts messages before they are delivered to a user's device. Adoption of TLS ranged from 14% (online retailers and News 50) to 52% (OTA Members), with most sectors in the 35% range.

DOMAIN LOCKING

Domain locking became a scoring element in 2013 due to its importance in prevention of domain takeovers (a penalty is assigned if the domain is not locked). More than 94% of organizations across all sectors lock their domains. The FDIC 100 leads at 97%, and the IoT 50 trails at 88%, indicating that several dozen sampled sites still need to lock their domains to help protect their brand and users from account takeover and domain abuse.

DOMAIN NAME SYSTEM SECURITY EXTENSION (DNSSEC)

DNSSEC adds security to the DNS lookup. It 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.

"Verisign is committed to the security and resiliency of the Internet. As the threat landscape evolves, it is necessary for organizations to implement responsible data security practices. It's a pleasure to partner with the OTA to raise awareness around these issues and continue our efforts in defending the Internet." – Danny McPherson, Senior VP and Chief Security Officer, VERISIGN

DNSSEC adoption remained flat this year, with only the Federal 50 having significant adoption (90%) in response to a Presidential directive. The only other sectors with any DNSSEC adoption are OTA members (5%), the News 50 (4%) and IoT 50 (4%). Broad implementation of DNSSEC continues to be hampered by lack of ecosystem infrastructure (hosting environments, registrars and browsers) as well as competition from higher priority security issues. Recognizing the complexity of implementing DNSSEC, bonus points were doubled in 2015.

SITE, SERVER & INFRASTRUCTURE SECURITY

A site's trustworthiness is largely defined by the security of the infrastructure. Users need assurance that the site and their data are secure. Proper implementation of best practices in this category also protects the site itself from attack.

Best practices in this category can be summarized as follows:

- Optimize SSL implementation using information gleaned from tools such as Qualys SSL Labs,[11] with specific focus on vulnerabilities that earn a letter grade of "F".
- Use EV SSL for brands and sites which are frequently spoofed and for sites where users need to be assured they are visiting and browsing a legitimate site.
- Implement AOSSL or HTTPS on all pages to maximize data security and online privacy.
- Implement a Web Application Firewall to monitor HTTP conversations and block common attacks such as cross-site scripting (XSS) and SQL injections.
- Proactively scan sites and third-party content for malicious links, iFrame exploits, malware and malvertising.[12]
- Implement bot detection and mitigation to help prevent brute force attacks, web scraping, account hijacking, unauthorized vulnerability scans, spam, and man-in-the-middle attacks.

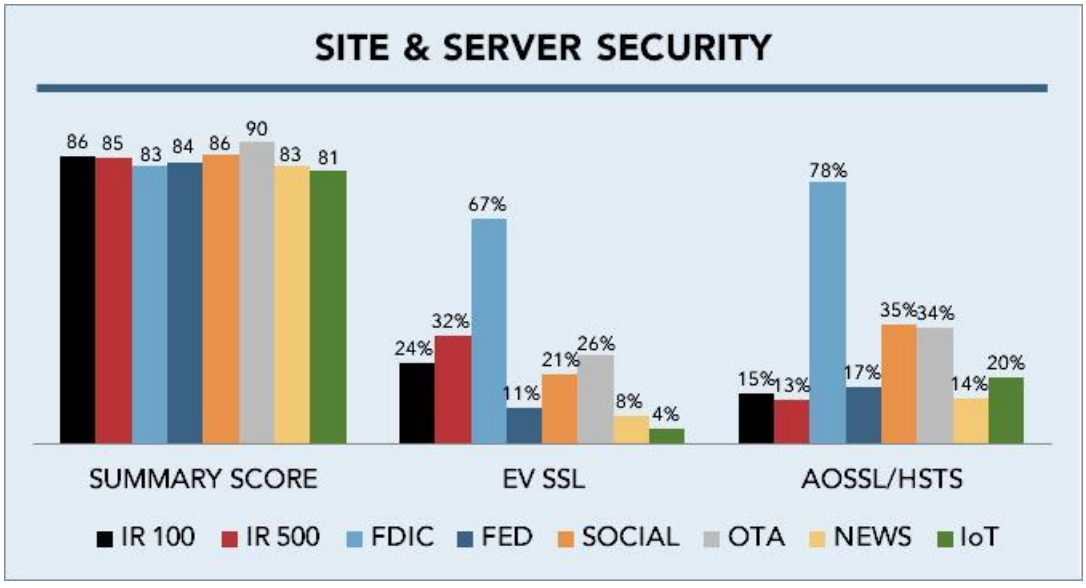

Figure 11 – Site & Server Security Scores/Adoption by Sector

[11] https://ota.ssllabs.com/
[12] https://otalliance.org/resources/type/advertising-integrity-fraud

As illustrated in Figure 11, the summary scores are in a relatively narrow range, while the adoption rate of key enhancements varies widely:

- SSL scores, which represent the base score in this category, are tightly concentrated around the overall average of 84.5 (vs. 83.4 last year).
- EV SSL adoption varies significantly across sectors – it is highest in the FDIC 100 (67%) and lowest in the IoT 50 (4%) and News 50 (8%).
- AOSSL helps ensure that data exchanged between the site and user is encrypted. Here, too, adoption varies – from 78% in the FDIC 100 to 13-17% for retailers, Federal 50 and News 50.

SERVER IMPLEMENTATION & VULNERABILITY ANALYSIS

Proper and ongoing SSL configuration is the primary mechanism sites can use to minimize vulnerabilities. While it is straightforward to obtain and install an SSL or EV SSL certificate, care must be taken to maintain a site properly, with ongoing checks to ensure that the latest protocols and configurations are in use. In the June 2015 SSL Pulse report, only 18.4% of the 146,708 sites tested were considered secure, a decrease from 28.4% in 2014.[13] Note that since the completion of the Audit, additional criteria have been added to the testing and scoring methodologies. Organizations are encouraged to review their sites against the new criteria and documented vulnerabilities.[14] [15]

"We endorse the work of the OTA and continue to work with industry to help develop best practices and educate those responsible for security to take steps to help protect against evolving threats. We're honored to be recognized once again on the OTA Honor Roll for practicing what we advocate." – Nicholas Hales, CEO, DigiCert

The SSL/Server scores incorporated data from DigiCert, Distil Networks, GlobalSign, High-Tech Bridge, Qualys SSL Labs, SiteLock and Symantec. Collectively the data was used to evaluate sites' SSL implementation, EV SSL adoption, and vulnerability to cross-site scripting, iframe exploits, malware, malicious links and bot exploits.

In addition to incorporating additional data attributes for the 2015 Audit, the OTA/SSL Labs tools and API upgraded the testing methodology to provide additional granularity. These enhancements provide better evaluation of server configurations against the current threat environment.[16] It is important to recognize that this analysis does not scan for every server attribute or possible combination of vulnerabilities. Secondly, in instances where more than one SSL server was found, the analysis focused on the highest scoring server.

---

[13] Source: Qualys 2015 report https://www.trustworthyinternet.org/ssl-pulse

[14] May 21, increased penalty for RC4, Logjam exploit and weak DH parameters https://community.qualys.com/blogs/securitylabs/2015/05/21/ssl-labs-117-obsolete-crypto-rc4-and-logjam

[15] May 22, increased penalty for TLS 1.2 https://community.qualys.com/blogs/securitylabs/2015/05/22/ssl-labs-increased-penalty-when-tls-12-is-not-supported

[16] https://community.qualys.com/blogs/securitylabs/2014/01/21/ssl-labs-stricter-security-requirements-for-2014

The additional granularity allowed analysis of unpatched vulnerabilities as well as adoption of security-related practices, and yielded the following observations:

- A significant fraction of overall sites remain vulnerable to well-documented and unpatched vulnerabilities. Though patches are available, 80% remain vulnerable to the BEAST exploit, 22% to the Heartbeat exploit, 25% to RC4-based attacks and 3% to the POODLE exploit. Collectively, this underscores the need for ongoing review and audit of internal systems.
- Support of Forward Secrecy (protection of public keys) for evaluated sites is lagging when compared to the latest SSL Pulse Report analysis of nearly 150,000 sites[17] – 60% of overall sites have no support (*vs.* 35% in the SSL Pulse Report), 13% have some support (*vs.* 36%), 17% support modern browsers (*vs.* 13%) and 10% support most browsers (*vs.* 16%).
- 51% of sites have already upgraded their SSL certificates to SHA-2 cryptographic hash functions, whereas 49% remain exposed.

As in previous years, the 2015 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. Several sites were able to reconfigure servers to reduce vulnerabilities, and while notification may have resulted in a favorable impact on a site's score, OTA felt responsible to notify the sites immediately to help protect the organizations and their customers from harm.

Presence of malicious links and malware was not found on any sampled sites, though XSS/iframe vulnerabilities were observed on nearly 8% of sites, including nearly half of the News 50 and one-fifth of the Federal 50. Overall this reflects increased diligence of site owners regarding scanning and securing their server configuration, though some sectors need to focus on this area and address vulnerabilities. Use of a web application firewall can help block attacks on these vulnerabilities – overall, 35% of sampled sites had a web application firewall, led by the Internet Retailer Top 100 (47%) and the Federal 50 (46%), while the Social 50 had the lowest adoption rate (12%). Sites which accept and rely on third-party content and advertising are also encouraged to hold their ad partners accountable to security best practices.

Increasingly, sites' vulnerabilities are being targeted by bot-orchestrated exploits as criminal networks leverage computing power for their illicit gain. Along with the proliferation of bot attacks, the severity and damage of these attacks has similarly increased. While earlier bot attacks were largely regarded as a nuisance, today's bot attacks can paralyze website infrastructure, pirate entire online directories, and destroy a company's competitive advantage. Meanwhile, beneficial bots such as Googlebot perform necessary tasks, but create false positives and confusion for Web Application Firewalls and Proxy services. In order to combat these alarming trends, companies should consider reinforcing their security strategy with the addition of proactive bot detection and mitigation solutions. Overall adoption of this practice is 86% with individual sector adoption ranging from 64% to 98%.

[17] Source: Qualys 2015 report https://www.trustworthyinternet.org/ssl-pulse/

SITE & SERVER SECURITY SITE SECURITY SCORES				
	2012	2013	2014	2015
Internet Retailer Top 100	75.9	85.3	81.9	85.7
Internet Retailer Top 500	76.8	85.1	83.3	85.3
FDIC 100	75.8	85.0	86.5	83.0
Federal 50	67.7	73.2	70.5	83.6
Social 50	77.7	82.1	86.2	86.1
OTA Members	79.8	87.1	86.8	89.8
News 50	-	-	83.2	83.0
IoT 50	-	-	-	81.3

Figure 12 – Site Security Score Average by Sector

As shown in Figure 12, year-to-year site security scores varied by sector, rising significantly in the Federal 50 (70.5 to 83.6). Modest growth was observed in some sectors (online retailers, OTA members), while others were flat (Social 50, News 50) or even dipped (FDIC 100). This variation emphasizes the importance of keeping pace with the latest protocols and SSL configuration settings.

Site administrators are encouraged to review the SSL Server Rating Guide,[18] updated in May, 2015, which provides an overview of the assessment methodology and addresses common configuration issues. A useful companion document is "SSL/TLS Deployment Best Practices" published by Qualys.[19] OTA's experience with these resources and tools has shown that changes can usually be made quickly and inexpensively once technical decision makers are engaged and issues are identified.

In addition to results from the Qualys SSL Labs tool, OTA also examined the type of SSL certificate utilized by the audited sites – Domain Validation (DV), Organization Validation (OV) and EV (Extended Validation) – which have widely varying methods for validating the identity of the entity receiving the certificate. The official name and location of entities purchasing OV and EV certificates are verified and confirmed directly with the entity by certificate authorities and are included in the certificate. By contrast, DV certificates are typically verified and confirmed through an automated process, making them more efficient and less expensive, but also more at risk for abuse. There are documented cases of "lookalike" SSL certificates (e.g., www.pay.pal-account.com) issued using DV, so a best practice is to use at minimum an OV certificate. The Audit found that 16% of sites use DV certificates, 53% use OV and 31% use EV.

EXTENDED VALIDATION SSL CERTIFICATES

Adoption of Extended Validation SSL Certificates (EV SSL) was introduced in the 2006 report due to its ability to address lookalike and phishing sites as well as fraudulently obtained certificates. EV SSL requires a verification and audit process that helps prevent deceptive entities from obtaining a certificate. EV SSL provides differentiation by displaying a green visual trust indicator in the address bar or browser chrome.

[18] https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide.pdf
[19] https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices.pdf

As illustrated in Figure 13, adoption of EV SSL certificates continues to increase, growing more than 19% to nearly 124,000 deployed certificates.[20] Growth has been attributed to brands' desire to instill consumer trust and increased differentiation, amplified by increased number of deceptive websites.

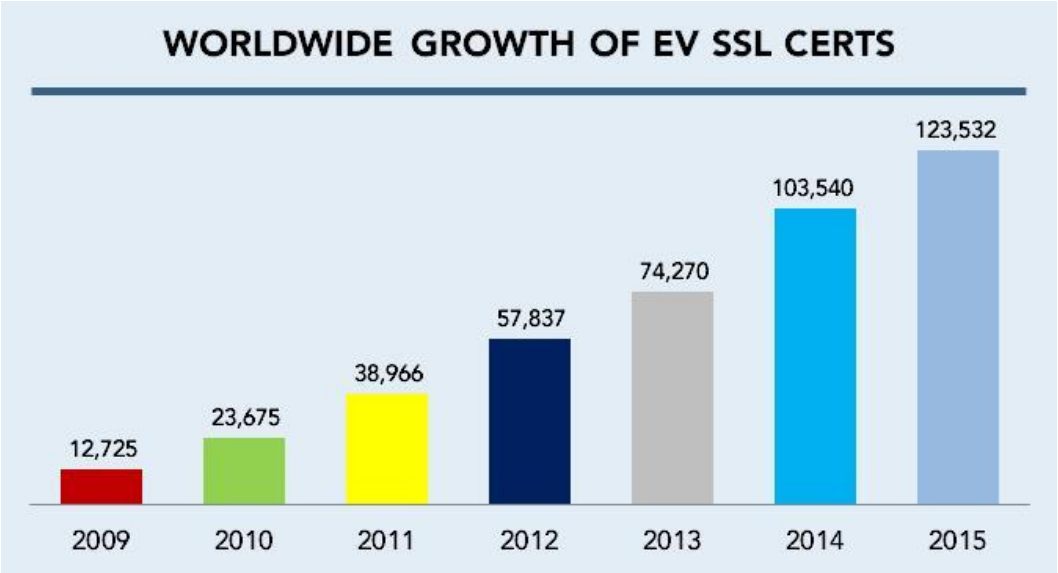

Figure 13 – Worldwide EV SSL Certs, April 2009-April 2015 (Netcraft, 2015)

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 all sectors but the FDIC 100 and News 50 showed a drop in adoption this year. Primary factors include the shift in specific organizations comprising each sector, (retailers), more sites adopting SSL within a sector while the absolute number of EVSSL certificates remained constant (Federal 50) and OTA members), and sites not renewing, (Social 50). As in past years, the FDIC 100 leads adoption at 67% (more than double the next closest sector), which reflects their need to combat lookalike sites used to attack banking customers.

SITE & SERVER SECURITY
EV SSL CERTIFICATE ADOPTION

	2012	2013	2014	2015
Internet Retailer Top 100	27.2%	28.0%	30.0%	24.0%
Internet Retailer Top 500	30.7%	33.4%	35.0%	32.1%
FDIC 100	55.0%	60.0%	64.0%	67.0%
Federal 50	25.9%	15.2%	12.5%	10.6%
Social 50	29.6%	24.5%	30.2%	20.8%
OTA Members	43.4%	35.0%	36.7%	30.0%
News 50	-	-	6.1%	8.1%
IoT 50	-	-	-	4.3%

[20] Source: OTA analysis completed April 15 – May 15, 2015 utilizing data from Netcraft published report. http://www.netcraft.com.

Figure 14 - EV SSL Certificate Adoption by Sector

DATA PROTECTION, PRIVACY & TRANSPARENCY

As businesses throughout the world are becoming "data driven" marketers and increasingly collecting and appending data through data brokers, and collection methods cross devices, it is more important than ever for organizations to strike the balance between data collection privacy and data stewardship. OTA has been advocating for increased transparency and discoverability of privacy policies since 2009, including recommending that policies provide clear disclosure of data collection, data usage, sharing and retention practices.

Best practices can be summarized as follows:

- Publish discoverable, easy to find, and comprehensible privacy policies.
- Create a layered, concise summary linking to an expanded policy. Use icons to help consumers navigate the policy elements more easily. Provide a clear statement including details if, what and for what purposes personal data is being shared with third parties. See OTA short form, linking to the full policy – http://otalliance.org/privacy-policy.
- 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/politica-de-privacida.
- Share details of data retention policies including clarification if such data is retained after the online interaction is terminated.
- 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.*"[21]
- Utilize tag management systems or privacy solutions that can manage third-party trackers and ensure they are acting properly.
- Disclose whether the site honors Do Not Track (DNT) settings in the site's privacy policy, and preferably honor users' DNT browser settings. Example copy –

  > *OTA respects enhanced user privacy controls. We support the development and implementation of a standard "do not track" browser feature, which is being designed to provide customers with control over the collection and use of information by third parties regarding their web-browsing activities. At this time OTA does not respond to DNT mechanisms. Once a standardized "do not track" feature is released, OTA intends to adhere to the browser settings accordingly.*

[21] Sites should conduct a legal review to ensure this draft copy is applicable to their site and business models.

As itemized in the Methodology & Scoring section, in addition to the bonus opportunities introduced last year (layered policies, disclosure of Do Not Track policy, use of tag management or privacy solutions), use of icons and support of multi-lingual policies were also awarded bonus points this year. These emerging best practices add to the analysis of privacy policies, third-party site tracking, honoring of DNT and data loss incidents or FTC privacy-related settlements/judgments evaluated in previous reports. By looking comprehensively across these criteria, it is possible to get a complete view of an organization's commitment to privacy.

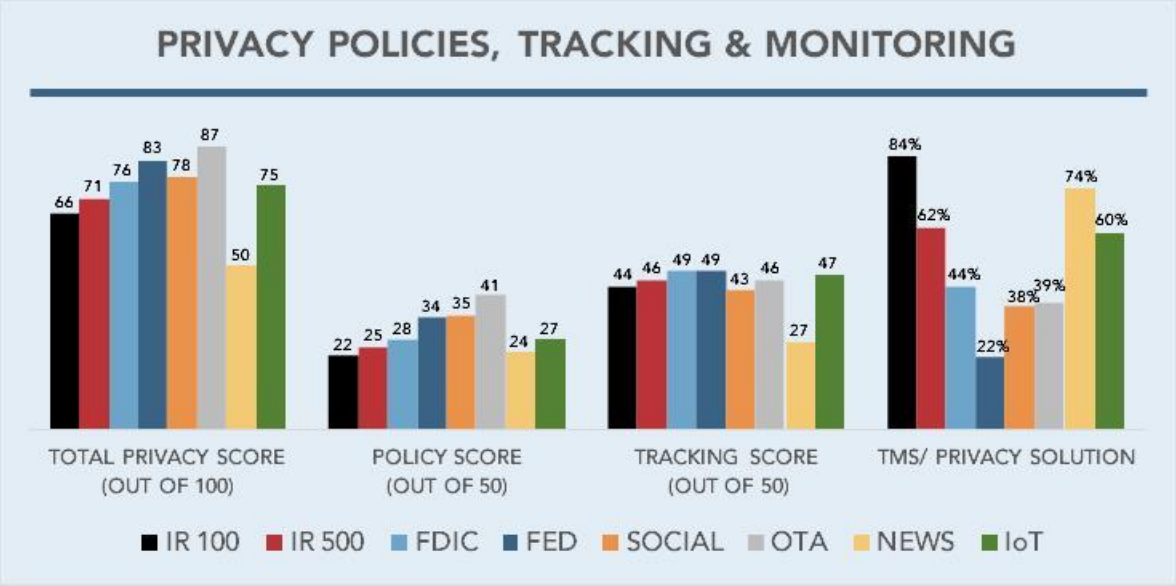

Figure 15 – Privacy Policy Scores and Monitoring by Sector

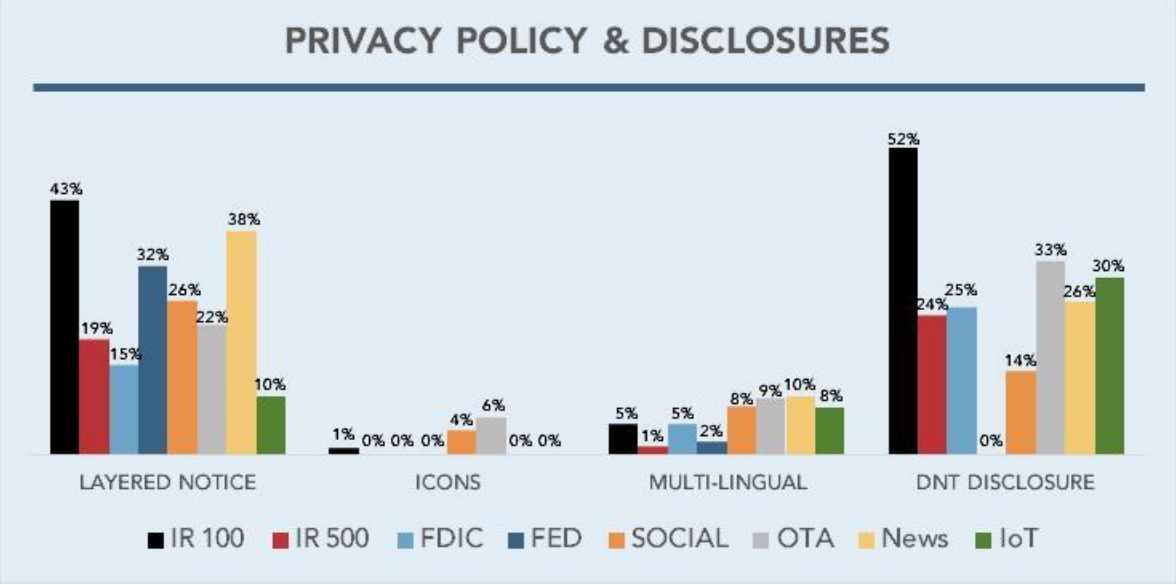

Figure 16 – Privacy Policy Implementation and Disclosure by Sector

Figure 15 shows the average privacy scores (including the two primary components scoring the privacy policy itself and third-party tracking used on the site) as well as adoption of tag management or privacy solutions in each sector. Figure 16 shows adoption rates of emerging best practices for each sector. Scores and adoption of various practices varied widely across sectors. Each area is addressed below.

PRIVACY POLICIES & THIRD PARTY TRACKING

Analysis of sites' core privacy policies and third-party tracking on sites was conducted by OTA and complemented by data from TRUSTe and AVG Technologies. Sites were scored 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. It should be noted that sites may have add-ons or apps which collect and share data that may not have been detected in this analysis.

Privacy scores averaged 72.9 across all sectors (vs. 64.7 last year), largely due to significant improvements by online retailers and the FDIC 100 (from 64 to 71 and 60 to 76 respectively) as well as the addition of the Federal 50 and IoT 50, which each had strong scores (83 and 75 respectively). Scores ranged from OTA members at 87 to the News 50 at 50. Overall, 23% of organizations had failing privacy scores (*vs.* 33% last year), with the biggest impact on the News 50 (50%), online retailers (27%) and IoT 50 (27%), indicating a need for intense focus on privacy policies and tracking in these sectors.

As seen in Figure 15, scores for the privacy policy component (worth 50 points) varied widely across sectors – low scoring was primarily due to lack of data retention disclosure and notice of data sharing. Third-party tracking scores were clustered near the 50-point maximum with the exception of the News 50 (27) which relies heavily on third-party advertising to drive revenue.

LAYERED NOTICE, ICONS & MULTI-LINGUAL POLICIES

In addition to the examination of privacy policies for layered notices introduced in 2014, new to the 2015 Audit was the examination of privacy policies for the use of icons and multi-lingual policies. Adoption of layered notice grew dramatically this year (21% overall *vs.* 11% last year), increasing at least three-fold for online retailers, the Social 50 and News 50. The newly evaluated Federal 50 had a strong showing with 32% adoption. This is moving toward an established best practice and may be incorporated into base scoring in future audits. Use of icons to assist navigation is almost non-existent in all sectors, with many at 0%. Support of multi-lingual privacy policies is in the early stages (average of 4% across sectors, ranging from 1% for online retailers to 10% for the News 50).

DO NOT TRACK DISCLOSURE & POLICY

As Do Not Track (DNT) becomes a legal requirement in some jurisdictions and issues regarding implementation are resolved, it becomes increasingly important for sites to both disclose their DNT policy as part of their privacy policy and to honor the browser's DNT setting as users visit the site.

Overall disclosure of DNT policy grew from 13% last year to 23% this year, led by the Internet Retailer Top 100 (52%) and with most sectors clustered in the 25%-35% range. The Social 50 lags in DNT disclosure

with only 14% adoption. Even with the growth since last year, because this requirement is now mandated by the State of California for all sites with users who reside in the State, the lack of adoption reflects a significant compliance concern. Honoring of browsers' DNT setting is even lower (1% across all sectors), with the majority of the adoption by online retailers (2%).

USE OF TAG MANAGEMENT SYSTEMS OR PRIVACY SOLUTIONS

Sites which rely on advertising and third-party analytics are faced with a complex and dynamic challenge of managing third-party tracking, which can create conflict with the stated privacy policy and regulatory compliance. Tag management and privacy solutions are becoming a best practice to allow review and monitoring of data collection and sharing in real time. OTA utilized site scanning capabilities to detect such systems and awarded bonus points if they were present.[22] [23]

Overall adoption of such solutions rose from 42% last year to 55% this year, indicating this is a well-adopted practice that will likely transition to part of the baseline scoring in future years. The Internet Retailer Top 100 led adoption (84%), followed by the News 50 (74%). Lowest adoption was in the Federal 50 (22%), likely due to the fact that they do not have many third-party trackers to manage.

WHOIS REGISTRATIONS

When a company registers a domain name, the Internet Corporation for Assigned Names and Numbers (ICANN) requires businesses to submit contact information including names, address, email and phone numbers. This information is posted in the WHOIS database which is available to anyone who chooses to find information about the owner of a site, providing the site owner has not made the registration information private. Fortunately, 91% of the sampled registrations are public (down from 96% last year). The largest sectors with private WHOIS registrations are online retailers and the FDIC 100 (each with 11% private registrations). Use of private registrations limits consumers' ability to discover who the owner of a site is, impedes transparency and reduces consumer trust.

DATA BREACH INCIDENTS & FTC SETTLEMENTS

Though even organizations with strong practices are not immune to compromise, data breaches and FTC settlements can be indicative of poor data stewardship and privacy practices, impacting a site's brand reputation and trustworthiness. Sites with such incidents or settlements receive a penalty impacting their overall composite score.

Data breach incidents occurred in 32 (4%) of the evaluated organizations (down from 58 total incidents last year), impacting all but the OTA sector. The FDIC 100 had the highest rate (9%) followed by the Social 50 (8%), while the News 50 was the lowest (2%). Due to its impact on consumer trust, the penalty for a breach was tripled this year. Five organizations (all online retailers) received a penalty for FTC suits or settlements this year (vs. only one retailer last year).

---

[22] Scanning capabilities provided by OTA member Ensighten, www.ensighten.com.
[23] Note while the presence of such solutions were verified, it is possible sites may not use the solutions or data.

CONCLUSION

The security and privacy landscape continues to evolve with new and innovative data driven services being introduced daily while data breaches and privacy missteps have become commonplace. As mobile devices and systems become more interconnected, our critical infrastructure, computers, mobile devices and applications are increasingly at risk.

These highly public failures and vulnerabilities have a negative impact on consumer trust. Left unchecked and without a commitment to meaningful self-regulation and enforceable codes of conduct, the reputation of brands and the health of the Internet itself is at risk. As the world economy and society at-large become increasingly reliant on the Internet, it is incumbent on the business community and associated trade organizations to embrace these practices and move from a compliance mindset to one of stewardship.

The OTA Online Trust Audit and Honor Roll highlights best practices, identifying companies who have demonstrated a commitment to consumer safety, security and privacy. Companies that earned Honor Roll status serve as a North Star for others to aspire to.

Adoption of the outlined best practices serves as the foundation of meaningful self-regulation. Companies who adopt these and others' security controls should be afforded protection from onerous regulatory oversight and receive "safe harbor" from frivolous lawsuits. In the absence of such commitment to consumer protection, Congress is increasing their demand that industry be accountable.[24]

The 2015 report confirms a renewed commitment to stewardship and adoption of best practices. This report serves four primary objectives:

- Promote best practices and provide tools and resources to assist companies in enhancing their security, data protection and privacy practices.
- Recognize leadership and commitment to best practices which aid in the protection of online trust and confidence in online services.
- Raise awareness of the risks, helping businesses to improve their security and privacy practices.
- Assist 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.

Updates to the report with additional data are posted at https://otalliance.org/HonorRoll. To submit comments or suggestions, email editor @ otalliance.org.

[24] U.S. Senate Hearing Online Advertising & Hidden Hazards to Consumer Security & Data Privacy
http://www.hsgac.senate.gov/hearings/online-advertising-and-hidden-hazards-to-consumer-security-and-data-privacy

ACKNOWLEDGEMENTS

The 2015 Online Trust Audit has been powered in part by leading organizations, including: Agari, AVG Technologies, DigiCert, Disconnect, Distil Networks, Ensighten, GlobalSign, High-Tech Bridge SA, IID, Microsoft, Qualys, Return Path, SiteLock, SSL Labs, Symantec, ThreatWave, TRUSTe and VERISIGN.

ABOUT ONLINE TRUST ALLIANCE (OTA)

The Online Trust Alliance (OTA) is a non-profit with the mission to enhance online trust and user empowerment while promoting innovation and the vitality of the Internet. Its 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, and meaningful self-regulation and data stewardship. Its members and supporters include leaders spanning public policy, technology, e-commerce, social networking, mobile, email and interactive marketing, financial, service provider, government agency and industry organization sectors.

OTA is a 501(c)(3) tax exempt global non-profit focused on enhancing online trust with a view of the entire ecosystem. OTA is supported by donations and support across multiple industries, representing the private and public sectors. To support OTA, visit https://otalliance.org/donate.

R11-17

APPENDIX A – 2015 HONOR ROLL RECIPIENTS

2015 Internet Retailer Top 500 – Honor Roll

1-800 Contacts Inc.
AAFES
AC Lens
Adobe Systems Inc.
② AJ Madison Inc.
④ Alibris Inc.
② Allied Electronics
④ Amazon.com Inc.
American Girl LLC
④ **American Greetings Corp.**
AmeriMark Direct LLC
Amway
④ Ancestry.com Inc.
APMEX Inc.
ASOS.com Ltd.
AutoZone Inc.
Avon Products Inc.
BabyAge.com Inc.
Balsam Brands
② Bare Escentuals Inc.
BarnesandNoble.com
BCBG Max Azria Group LLC
Beachbody LLC
bebe stores Inc.
③ Bellacor Inc.
③ Best Buy Co. Inc.
④ Big Fish Games Inc.
④ BikeBandit.com
BJ's Wholesale Club
Boden USA
Bonobos
Brooks Brothers
③ Build.com Inc.
③ BuildASign.com
BuildDirect Technologies Inc.
Burberry Ltd.
④ **Cabela's Inc.**
Charlotte Russe Inc.
Chegg Inc.
② Christianbook.com LLC
Coach Inc.
② Coastal Contacts Inc.
Colony Brands Inc.
Columbia Sportswear Co.
Costco Wholesale Corp.
CPO Commerce LLC
Crutchfield Corp.
④ CustomInk
Destination XL Group Inc.
Diamond Nexus
② Dillard's Inc.
Discount Dance Supply
③ DiscountRamps.com LLC
③ Disney Store USA LLC
Dollar Shave Club
② DoMyOwnPestControl.com
Drs. Foster and Smith
DSW Inc.
eBags Inc.
Eddie Bauer LLC
Edible Arrangements
Entertainment Earth Inc.
eSalon
Estee Lauder
③ Etsy Inc.
③ evo
② Express Inc.
Fanatics Inc.
④ Fathead LLC
Forever 21
Fossil Inc.
FreshDirect LLC
③ GameFly Inc.
④ **GameStop Corp.**
Gap Inc.
Gilt Groupe
Golfsmith International
Hallmark Cards Inc.
Hammacher Schlemmer
Hanna Andersson Corp.
④ Hayneedle Inc.
Hot Topic Inc.
④ HSN Inc.
③ Hulu LLC
③ Ice.com
② ID Wholesaler
iHerb Inc.
IKEA.com
③ JackThreads.com
Jenson USA
JimmyJazz.com
Joann.com
Jomashop.com
K&L Wine Merchants
③ Karmaloop.com
Kate Spade
Keurig Green Mountain Inc.
Lamps Plus Inc.
LD Products
LifeWay Christian Resources
③ **LivingSocial Inc.**
Luxottica Group S.p.A.
Macy's Inc.
Mason Companies Inc.
MEC
④ Microsoft Corp.
③ Minted
④ ModCloth Inc.
Monoprice Inc.
Musician's Friend Inc.
NAPA

Bold – OTA 2015 Honor Roll Top 10 Retailer ② ③ ④ – Number of consecutive years as an Honor Roll

2015 Internet Retailer Top 500 – Honor Roll, continued

National Builder Supply
National Football League
National Hockey League
NBTY Inc.
② Nebraska Furniture Mart
Neebo Inc.
④ **Netflix Inc.**
③ New Balance
② Newegg Inc.
② Nike Inc.
Nine West Holdings Inc.
② Nordstrom Inc.
Northern Tool & Equipment
Nuts.com
OmahaSteaks.com Inc.
Online Stores Inc.
OpticsPlanet Inc.
Orchard Brands Corp.
② OvernightPrints.com
④ Overstock.com Inc.
③ Pacific Sunwear
Pandora
Parts Express
Party City Corp.
④ Payless ShoeSource Inc.
④ PersonalizationMall.com
Petco Animal Supplies Inc.
PetSmart Inc.
Philips Electronics N.V.
Pier 1 Imports Inc.
Planet Shoes
PrintingForLess.com Inc.
② PromGirl LLC
Purchasing Power LLC
PureFormulas.com
QVC Inc.
③ Ralph Lauren Media
Real Real Inc.
RealTruck.com
Redbox Automated Retail
REI
Rent the Runway Inc.
RepairClinic.com Inc.
③ Replacements Ltd.
Rock Bottom Golf
③ RockAuto LLC
Sears Holdings Corp.
③ Sephora USA Inc.
Shindigz
Shoebuy.com Inc.
ShopLadder
ShoppersChoice.com
② Signet Jewelers Ltd.
Skechers USA Inc.
Smarthome Inc.
④ Sonic Electronix
Spanx Inc.
② **SparkFun Electronics**
Sports Authority
Spotify
② Spreadshirt Inc.
Stroll LLC
Stuart Weitzman LLC
② Sweetwater
③ SwimOutlet.com
Tempur-Pedic
The Children's Place
The Clymb
The Finish Line Inc.
The Grommet
④ The Gymboree Corp.
The Honest Company Inc.
③ The Lakeside Collection
The Orvis Co. Inc.
④ ThinkGeek Inc.
③ Threadless.com
④ Tiffany & Co.
Tilly's Inc.
Tire Rack Inc.
TJX Cos. Inc.
TOMS Shoes Inc.
③ Tory Burch LLC
Touch of Modern Inc.
② Tumi Inc.
Turn5 Inc.
Ulta Beauty
UnbeatableSale.com Inc.
② Under Armour Inc.
Uniqlo USA Ltd.
VF Corp.
② Vintage Tub & Bath
VitaminShoppe.com
④ Walmart.com
Warby Parker
③ Wayfair LLC
③ Weight Watchers
West Marine Products
Yoox Group
Zazzle Inc.
③ zulily Inc.
Zumiez Inc.

Bold – OTA 2015 Honor Roll Top 10 Retailer ② ③ ④ – Number of consecutive years as an Honor Roll recipient

2015 FDIC Top 100 Banks – Honor Roll

- ④ American Express Bank, FSB.
- ④ American Express Centurion Bank
- ② Arvest Bank
- ④ Bank of America California, National Association
- ④ Bank of America, National Association
- ④ BMO Harris Bank National Association
- ② Branch Banking and Trust Company
- Capital One Bank (USA), National Association
- Capital One, National Association
- Chase Bank USA, National Association
- CIT Bank
- ③ Citibank, National Association
- ② City National Bank
- Comerica Bank
- Commerce Bank
- Compass Bank
- Deutsche Bank Trust Company Americas
- Discover Bank
- ③ E*TRADE Bank
- ② EverBank
- ② Fifth Third Bank
- First Hawaiian Bank
- First Niagara Bank, National Association
- First Republic Bank
- First-Citizens Bank & Trust Company
- ④ Frost Bank
- GE Capital Bank
- Iberiabank
- ② JPMorgan Chase Bank, National Association
- ③ Morgan Stanley Bank, National Association
- ③ Morgan Stanley Private Bank, National Association
- MUFG Union Bank, National Association
- PNC Bank, National Association
- ② Regions Bank
- ④ Scottrade Bank
- State Farm Bank, F.S.B.
- Synovus Bank
- TCF National Bank
- TD Bank USA, National Association
- TD Bank, National Association
- The Huntington National Bank
- ④ U.S. Bank National Association
- ③ UBS Bank USA
- ④ **USAA Federal Savings Bank**
- Valley National Bank
- ④ Wells Fargo Bank, National Association

2015 U.S. Federal Government Top 50 – Honor Roll

- Census Bureau
- Centers for Disease Control and Prevention (CDC)
- Dept of Education
- Dept of Energy
- Dept of Health & Human Services (healthcare)
- Dept of Interior
- Dept of State
- Dept of Transportation
- Federal Bureau of Investigation (FBI)
- **Federal Deposit Insurance Corporation (FDIC)**
- Federal Trade Commission (FTC)
- First Gov (USA.gov)
- General Services & Administration (GSA)
- House of Representatives
- National Aeronautics and Space Admin (NASA)
- National Institutes of Health (NIH)
- National Park Service (NPS)
- Social Security Administration (SSA)
- U.S. Government Jobs
- US Postal Service
- White House

Bold – Top score within sector ② ③ ④ – Number of consecutive years as an Honor Roll recipient

2015 Social Top 50 – Honor Roll

- ❸ AOL
- ❹ Badoo.com
- ❸ Blogger
- ❷ Box
- Craigslist
- ❷ Dropbox
- ❸ eHarmony
- ❹ Facebook
- ❸ FiveRR
- Flickr
- ❸ Foursquare
- ❸ Goodreads
- Google Docs
- ❷ iCloud
- ❸ Instagram
- ❹ LinkedIn
- Match.com
- ❷ MySpace
- ❸ Pinterest
- ❸ PlentyofFish
- QQ.COM Pengyou
- Tagged
- ❹ Tumblr
- ❹ **Twitter**
- ❸ Wordpress
- ❷ Yahoo!
- ❸ YouTube
- Zoosk
- ❹ Zynga

2015 News/Media Top 50 – Honor Roll

- **Business Week**
- ❷ Google News
- ❷ New York Times
- Weather.com

2015 Internet of Things Top 50 – Honor Roll

- ADT
- Alarm
- Basis
- **Dropcam**
- Jawbone
- Nest
- Nike
- Phillips
- Wink
- Withings

Bold – Top score within sector

❷ ❸ ❹ – Number of consecutive years as an Honor Roll recipient

2015 OTA Members – Honor Roll

- ③ ACT
- ② Act-On Software
- ④ AG Interactive
- ④ Agari
- ② AVG Technologies
- BaseGrow
- Brand Protect
- CertainSource
- ② Coles
- ③ comScore
- ④ Constant Contact
- ④ DigiCert
- Disconnect
- ② Distil Networks
- ③ eBay Enterprise
- ④ eHarmony
- ④ Ensighten
- ④ Epsilon
- ④ Exact Target
- ② Flybuys
- Gap
- ④ GetResponse
- ④ Global Sign
- ④ GoDaddy
- ④ Harland Clarke Digital
- ④ High-Tech Bridge SA
- ④ Iconix
- ④ Identity Guard
- ③ IID
- ④ Innovyx (Javlin Marketing Group)
- ④ Intersections
- Kromtech Alliance Corp.
- ② LashBack
- LifeLock
- ③ Listrak
- Malwarebytes
- ④ Mark Monitor
- ④ Marketo
- Maropost
- ② MeetMe
- ③ Message Systems
- ④ Microsoft
- ④ Online Trust Alliance
- ② Optizmo
- Oracle
- Oracle (Responsys)
- ④ Publishers Clearing House
- ④ Return Path
- ③ RiskIQ
- ④ Sailthru
- ④ Silverpop
- Simpli.Fi
- ③ SiteLock
- ④ Symantec
- ② The Media Trust
- ③ ThreatWave
- ④ TRUSTe
- ④ TrustSphere
- ④ **Twitter**
- UnsubCentral
- ③ VERISIGN
- ③ Vivaki
- ② WebMD
- ③ ZEDO

Bold – Top score within sector

② ③ ④ – Number of consecutive years as an Honor Roll recipient