Summary
Now in its 14th year, National Cyber Security Awareness Month (NCSAM) – co-founded and led by the National Cyber Security Alliance (NCSA) and the U.S. Department of Homeland Security (DHS) – generated unmatched, far-reaching results across industry, diverse organizations, government, the military and academia. NCSAM 2017’s primary goal was to raise extensive awareness and empower everyone online to be safer, more secure and better able to protect their personal information by taking simple, actionable steps. The month’s theme – “Our Shared Responsibility” – emphasized the role each individual plays in promoting a more trusted internet and was reinforced consistently throughout October and beyond. NCSAM 2017 yielded many noteworthy and impactful successes, and this report shares both quantitative and qualitative results for the month.

Perhaps one of NCSAM 2017’s most striking achievements was the tremendous adoption and the sharing of key messages and advice. Whether it was linking NCSAM and October to pumpkin spice, showcasing the overarching “Our Shared Responsibility” theme, the widespread use of NCSA-created materials or the promotion of our partners’ programs, the organic growth was unprecedented. The following highlights several significant examples:

Just prior to the month, Bloomberg’s Privacy and Data Security blog announced NCSAM – tying it in a consumer-friendly way to other cultural October traditions like Halloween and the return of pumpkin spice snacks and treats. This article by nationally syndicated columnist, Michelle Singletary, also positioned NCSAM alongside Halloween with tips directed at seniors on how to protect their social security benefits from hackers.

A variety of organizations, including Cisco (a NCSA board member company), demonstrated strong, month-long alignment by developing helpful resources, blogs, webinars and live events designed to help employees meet their most pressing cybersecurity challenges.

Partner engagement strengthened significantly as exemplified by press releases referencing “National Cyber Security Awareness Month” that were created and distributed during September, October and November. These partner-generated, NCSAM-specific releases increased by 88% – from 43 in 2016 to 81 in 2017.

The Federal Bureau of Investigation (FBI) showcased October as an “important reminder of the need to take steps to protect yourself and your family when using the Internet.” Both NCSA and DHS were positioned as NCSAM leads, and images from NCSA’s “Our Shared Responsibility” infographic were used.
A variety of international stories ran throughout and post NCSAM. This feature from the U.S. Embassy in Zimbabwe addresses raising awareness about cybersecurity and the need for campaigns like Stop.Think.Connect.

As late as Nov. 29, the Harvard Business Review touted Facebook’s Hacktober as a model for other organizations to build and maintain a security-conscious culture. It also pointed out the critical role that third-party organizations like NCSA play in providing resources, support and content.

In an effort to broaden the scope and increase global support for NCSAM, NCSA and DHS extended the month’s reach beyond U.S. borders to include other countries committed to internet safety. Sharing already-created resources for American audiences, several international organizations, including the European Union Agency for Network and Information Security (ENISA), the Organization of American States (OAS) and the U.S. Department of State, translated STOP. THINK. CONNECT.™-inspired messaging and materials into various languages. For the first time ever, the month kicked off with a global launch at OAS’ headquarters in Washington, D.C., on Oct. 3. This event emphasized fostering a culture of cybersecurity as technology evolves. Topics included the international adoption of safe cyber practices, how to keep all global digital citizens safer and more secure online, how governments and the private sector can collaborate in their online safety efforts, and a look ahead to the benefits of a globally secure internet.

NCSA worked closely with its NCSAM partners and Champions to elevate the brand’s exposure in the U.S. and globally - building top international, national and local media mindshare that moved beyond the cybersecurity and privacy beats with consumer, business and lifestyle stories. Since last year, the month increased its quality and diversity of coverage with placements in NPR Marketplace, USA Today, CNBC, The Wall Street Journal, Gizmodo, Yahoo News, Huffington Post (U.S. and UK), International Business Times and other well-regarded national and international outlets.

Beating the drum, NCSA reinforced a media strategy that built momentum throughout the month and included:

- Pre-briefings in San Francisco and New York City for Michael Kaiser with top-tier outlets that established a “case” for NCSAM and paved the way for specific coverage of NCSAM activities and reactive media.
- Stakeholder ownership that inspired survey support and media participation, resulting in an increase of NCSAM stories internationally in Latin America, Africa and Europe.

The NCSAM 2017 Media Backgrounder – a toolkit that included fast facts, tips, resources and story ideas – was distributed to 2,000+ local markets and supported 2,446 articles about the month. A Champion version of the backgrounder was also created to ensure consistent messaging and theme alignment across events, press releases and other activities.

Many media outlets developed stories directly from the backgrounder. For example, This October, Revisiting Our Shared Responsibility To Stay Safe Online in Forbes discussed NCSA and DHS leadership behind the month and shared key STOP. THINK. CONNECT.™ tips. The article also referenced the international expansion of NCSAM 2017 and ways to get involved.

---

1 These 2,446 articles specifically referenced “National Cyber Security Awareness Month” in the story and were often aligned with NCSAM messaging and information included in the NCSAM Backgrounder.
New story angles with partner participation, including:
- continued, extensive use of the four weekly themes
- the top cyber concerns for consumers and small and medium-sized businesses
- teens and parents identifying fake news as a new online concern
- filling today’s global talent gap in cybersecurity
- securing the connected American home from hackers.

In addition to a highly strategic media plan, several additional elements elevated NCSAM’s exposure, reach and influence:

1,050 organizations registered as Champions. This is an increase of 21% over last year’s 870. The Individual Champions program also grew, with a total of 603 supporters in comparison to 432 in 2016 – an increase of 40%.

There was strong commitment from government throughout the month. Key influencers such as the FBI, Ready.gov, the Department of Energy, Small Business Administration and State Department were very active on social media, sharing NCSA materials and key messages for the weekly themes. Local and state government entities registered as Champions and implemented initiatives such as issuing official proclamations, hosting cybersecurity presentations for students, organizing food for thought truck rallies – in which customers were quizzed on their online safety knowledge – and creating NCSAM websites.

Participation also grew in higher education where student communications, articles and on-campus activities expanded awareness among vulnerable student populations. Many colleges and universities also designed their own NCSAM website content.

In October, 76 organizations registered as STOP. THINK. CONNECT.™ partners – bringing the total number of partners to 804 by the end of the month.

Stopthinkconnect.org experienced a 5% increase in page views in October 2017 compared to the previous year, with 72,524 views (compared to 68,843 last year).

The Week 1 Twitter chat held on Oct. 5 reached an all-time high for NCSA in potential reach (3,116,365).

NCSAM messaging continued to gain traction. “Stay Safe Online” was featured in hundreds of stories, and the overall reach² experienced a 121% increase in articles³ and 130% growth in unique viewers.⁴

The STOP. THINK. CONNECT.™ campaign was also shared far and wide by key institutions and partners, including the White House and United States Army, as well with influential media like Forbes, the HuffPost and Politico.

The NCSA and DHS teams met on Nov. 17 to capture “key learnings” for NCSAM 2018 planning and to review the month’s successes and areas for improvement. The integrated group discussed topics including the benefits of a high-profile, pre-launch initiative; the great draw of DHS leadership at events; continued exploration of venues for contributed content and blogs; fresh, innovative ideas for tactics; international support; increased partner engagement; creative weekly themes and the continued use of livestream and other social media tools to expand reach.

² Stay Safe Online = 1,754 articles and 1,956,030,672 unique viewers in 2017; 793 articles and 849,855,525 unique viewership in 2016.
³ For the purposes of this report, “articles” refer to original media coverage and do not include press releases or press release pickups.
⁴ “Unique viewers” refer to the number of individuals requesting pages from a website during a given month. This measurement of reach can be the result of original media articles or press releases that have been distributed. Meltwater, NCSA’s media intelligence platform, is provided these numbers by SimilarWeb - who took over as their metrics partner in January 2017. As a result of this new partnership between Meltwater and SimilarWeb, the 2016 NCSAM results were recalculated for this report to ensure fair and accurate year-over-year comparisons.
The meeting was extremely helpful and reminded both groups that, among other important points, early NCSAM planning is critical to continued growth and success. The results of that meeting are being shared internally with DHS staff.

This report shares a summary of results for the following:
- Full-court press
- “Newsworthy” highlights
- Digital and social media analytics
- Champions
- Key NCSAM weekly activities
- Collateral
- Stakeholder engagement

Full-Court Press
NCSA and DHS collaborated on a comprehensive media outreach plan – created for complementary traditional and social media opportunities. Beginning in February, bi-weekly planning calls were conducted, and from early July on, the calls were held on a weekly basis. Detailed notes, ongoing follow-up and discussion among call participants about the status of various activities, research, new partner initiatives and events – all with the goal of generating widespread media across a variety of platforms – contributed to a strategic, comprehensive plan. Both traditional and social media outreach was ongoing and leveraged a variety of story angles, including the weekly themes, local events, new research, complementary partner initiatives, reaction(s) to timely “headlines,” etc. NCSA and DHS also expanded the use of livestreaming at all events to dramatically extend the audience reach beyond those who were able to attend in person. The following summarizes media highlights and coverage:

Expanding its media footprint, NCSAM 2017 generated 2.4 billion+ or 2,400,149,313 unique views – an increase of 44% compared to last year – from print/digital stories and press releases that specifically mentioned National Cyber Security Awareness Month by name. Additional NCSAM activities (i.e., stakeholder initiatives, partner research, events with DHS, interviews with leadership, etc.) during the September, October and November timeframe resulted in 3.3 billion+ views that increased cybersecurity awareness and generated mass attention to the weekly themes.

NCSA leveraged a variety of tactics to promote October’s activities, including media briefings in San Francisco and New York City to meet with leading consumer and business reporters, a Radio Media Tour (RMT) and a press release that kicked off the month. Additionally, the NCSAM Media/Champion Backgrounder, weekly Twitter chats and Facebook Livestreams at events drove social engagement and high-profile media placements. NCSA also designed and distributed rich content in the form of thematic weekly press releases and a collection of infographics and memes for social and online engagement.

Media Reach
During the months of September, October and November, there were thousands of digital, print and broadcast stories that covered NCSAM. These stories included partner research, NCSAM weekly themes and related storylines. The following is a summary of noteworthy highlights:

Articles

---

5 2016 = 1,670,777,175 unique views. As a reminder, all 2016 metrics were recalculated to ensure accurate year-over-year comparisons with Meltwater’s new metrics partner, SimilarWeb.

6 3.3 billion+ = 3,304,394,053

7 2016 unique articles = 2,583
Broadcast
There were 479 broadcast features during the NCSAM timeframe, which reached an estimated audience of 7,726,555 nationwide. These stories exemplified the strong adoption of NCSAM’s weekly themes with localized segments discussing the cybersecurity workforce, consumer tips to stay safe online, advice for small businesses, the smart home and more. The number of broadcast segments decreased by 44% from 861 in 2016.

NCSA/Microsoft – Keeping Up with Generation App Survey: NCSA Parent/Teen Online Safety Survey
This second annual study – co-sponsored by Microsoft – was released during Week 3 and received widespread attention including three separate HuffPost articles and coverage in Psychology Today, CBS Radio and International Business Times. (Note: In 2016, the findings were released leading up to NCSAM at the end of August.)

Raytheon/Forcepoint and NCSA – Securing Our Future: Cybersecurity and the Millennial Workforce
A total of 46 articles and blogs about the Raytheon/Forcepoint and NCSA global study on millennials and the cyber workforce were published, resulting in 69 million+ unique viewers. Placements were featured in a variety of outlets, including VentureBeat, Wall Street Journal Cybersecurity Pro, HuffPost, Washington Business Journal, WTOP (Washington, D.C.), The National (UAE), CISO magazine and MSN (UAE).

Key Messages
Message alignment was strong across key terms. Critical NCSAM messages were included in hundreds of stories, countless press releases and in top regional and national outlets during September, October and November, including USA Today, CNN International, Business Insider, HuffPost, Forbes, Bloomberg, TechCrunch and The Guardian.

During NCSAM 2017, “Stay Safe Online,” “Keep a Clean Machine” and “Our Shared Responsibility” were featured extensively.

- **“Stay Safe Online”**: 1,754 articles representing a year-over-year increase of 121% (793 articles in 2016)
- **“Keep a Clean Machine”**: 119 articles, an increase of 89% (63 articles in 2016)
- **“Our Shared Responsibility”**: 77 articles, an increase of 126% (34 articles in 2016)

**“Newsworthy” Highlights**
Champions
The NCSAM Champion program allows individuals and organizations to officially show their support and

---

8 69 million+ = 69,112,328 unique viewers
engage in the month’s activities. They are critical to NCSAM’s success – driving promotion globally, locally and to their own audiences. Champions truly represent those dedicated to promoting a safer, more secure and more trusted internet. In 2017, 1,050 organizations – including academic, public and private organizations and government institutions – registered. This is an increase of 21% from last year's 870 Champions.

New for 2017 was the opportunity for Champion organizations to align their events as NCSAM Partner Events. They were provided a list of criteria to follow, including showcasing the “Our Shared Responsibility” theme, the month’s history and how to incorporate official NCSAM logos, graphics and other key messages. In a period of 24 hours following the announcement of this new opportunity, NCSA received 90 Champion registrations from organizations.

**Breakdown of Champion Organizations**

- Government: 92
- Industry: 531
- Higher education: 233
- Nonprofit: 109
- Trade association: 25
- K-12 education: 16
- Other: 43

Since the individual Champions program was launched in 2015, it has experienced promising year-over-year growth. In 2015, a total of 283 supporters signed up, followed by 432 in 2016. As of Oct. 31, 2017, 603 individuals had registered – an increase of 40% from the previous year.

**Social Media Success:**

Social media engagement grew this NCSAM, with the #CyberAware hashtag used 81,256 times in October 2017 (a 16% increase over last year). Additionally, 23,958 Twitter handles tweeted the #CyberAware hashtag during the month – a 13% increase over the number of people who tweeted with the NCSAM hashtag in 2016. The hashtag potentially reached 84,447,531 (a 24% increase over last year) and generated 599,818,668 potential impressions (a 22% increase over last year).

**Digital and Social Media Overview**

**Website Analytics for October 2017**

<table>
<thead>
<tr>
<th></th>
<th>2015 Visits</th>
<th>2016 Visits</th>
<th>2017 Visits</th>
</tr>
</thead>
<tbody>
<tr>
<td>StaySafeOnline.org</td>
<td>105,466</td>
<td>(22% decrease from 2016)</td>
<td>79,514</td>
</tr>
<tr>
<td>Page views</td>
<td>284,129</td>
<td>(4% increase)</td>
<td>22,500</td>
</tr>
</tbody>
</table>
stopthinkconnect.org
• Visits: 26,689 (7% decrease from 2016)
• Unique visitors: 20,203 (11% decrease)
• Page views: 72,524 (5% increase)

lockdownyourlogin.org (formerly lockdownyourlogin.com)
• Visits: 16,340 (75% decrease from 2016)
• Unique visitors: 14,325 (79% decrease)
• Page views: 32,736 (61% decrease)

NOTE: The lockdownyourlogin.org decreases can likely be attributed to the fact that the Lock Down Your Login site was originally launched in partnership with the White House prior to NCSAM 2016 and heavily promoted on social, digital and traditional media and public service announcements. The current site is now used for smaller-scale efforts to educate federal, state and local government officials and staff about online account security.

Blogs
NCSA published 32 posts to the Stay Safe Online blog in October 2017, including 18 guest submissions. The posts ranged in subject matter from cyberbullying in the workplace to parenting in the digital age to the importance of diversity in the cybersecurity workforce. The following organizations contributed guest posts to the Stay Safe Online blog during the five weeks of NCSAM: ADP; AT&T; CDK Global; Center for Cyber Safety and Education; Cisco; EDUCAUSE; Facebook; Jetico; Logical Operations; McAfee; Microsoft; SANS Security Awareness; TeleSign; UL.

Michael Kaiser also contributed five Q&A-style posts to his HuffPost contributor column during the month. The posts featured interviews with Eva Velasquez of the Identity Theft Resource Center, Lance Spitzner of SANS Security Awareness, Anthony Grieco of Cisco, Valerie Maclin of Raytheon, Carolyn Ford of Forcepoint and Ken Modeste of UL.

Webinars and Livestreams
Throughout October 2017, Michael Kaiser and other NCSA staff members participated in a number of webinars that were publicized and streamed to security professionals, small to medium-sized business owners, academic institutions and the general public.

• On Oct. 4 Michael joined the MS-ISAC’s national webinar; he shared the month’s themes, events and key dates, collateral schedule and discussed ways for partners and individuals to engage with 363 attendees.
• Oct. 10 marked the first Cybersecure My Business™ webinar, “Let’s Talk About Ransomware and Phishing.” The hour-long virtual event featured experts from government and industry and was extremely well received with close to 850 registrants and more than 500 highly engaged and enthusiastic online guests.
• NCSA also arranged and participated in an RSA® Conference virtual session on Oct. 19. Moderated by Michael, a panel of industry pros discussed “Can the Internet of Insecure Things Be Saved?” to an online audience of 143.
• As in previous years, Michael delivered opening remarks for the EDUCAUSE Live! webinar on Oct. 23. His welcome began with strong NCSAM messaging that was followed up by a guest speaker on security awareness in higher education. There were 130 attendees at this online event.

For the last two years, NCSA has been focused on reaching more individuals by implementing Facebook Live into key events and initiatives as part of regular NCSAM social media efforts. The total number of views for October 2017 to date is 20,745 – a 46% increase over October 2016 (14,137 views to date). NCSA attributes this to better promotion of upcoming broadcasts and the cybersecurity careers series during Weeks 4 and 5.
Social Media
In 2015, NCSA changed the official NCSAM hashtag to #CyberAware (in previous years, it had been #NCSAM) in an effort to make social media engagement more accessible during October and year-round. Over the last two years, the hashtag performed extremely well, and we have seen marked growth in 2017.

**CyberAware Usage**
- **September:**
  - Mentions: 12,563 tweets with #CyberAware (85% increase over 2016)
  - People: 4,737 Twitter users tweeted with the hashtag (111% increase)
  - Total potential reach: 17,789,273 (40% increase)
  - Total potential impressions: 86,865,327 (111% increase)

- **October:**
  - Mentions: 81,256 tweets (16% increase over 2016)
  - People: 23,958 Twitter users tweeted with the hashtag (13% increase)
  - Total potential reach: 84,447,171 (24% increase)
  - Total potential impressions: 599,818,668 (22% increase)

- **Nov. 1-3:** *(Note: The Twitter chat for Week 5 was held on Nov. 1)*
  - Mentions: 3,371 tweets
  - People: 1,565
  - Total potential reach: 7,048,890
  - Total potential impressions: 29,984,747

**ChatSTC Twitter Chat Series**
NCSA and STOP. THINK. CONNECT.™ (@STOPTHNKCONNECT) hosted six #ChatSTC Twitter chats in recognition of NCSAM, with the Week 1 chat (Oct. 5) hitting an all-time high for NCSA in potential reach (3,116,365).

**October**
- Mentions: 11,694 (19% decrease from 2016)
- People: 3,103 Twitter users tweeted with the #ChatSTC hashtag (1% increase)
- Total potential reach: 12,004,575 (28% increase)
- Total potential impressions: 168,335,045 (11% increase)

**Nov. 1-3**
- Mentions: 1,383 tweets
- People: 314 Twitter users tweeted with the #ChatSTC hashtag
- Total potential reach: 1,730,712
- Total potential impressions: 22,695,342

**October**
@StaySafeOnline Twitter Account
- Sent out 2,411 tweets (96% increase over 2016)
- Gained 1,616 followers (17% increase)
- Had a total engagement of 11,375 (29% increase)

@STOPTHNKCONNECT Twitter Account
- Sent out 1,854 tweets (51% increase from 2016)
- Gained 699 followers (0% increase)
- Had a total engagement of 4,160 (23% decrease)

NCSA Facebook Page
- Total reach: 276,525 (41% decrease from 2016)
- Impressions: 479,241 (46% decrease)

STOP. THINK. CONNECT.™ Facebook Page
Total reach: 47,102 (6% decrease from 2016)
Impressions: 70,873 (18% decrease)

NOTE: In 2016, Facebook changed its algorithm to de-emphasize organization pages. As a result, Facebook users are less likely to see NCSA’s (and any other organization’s) content. This explains, in part, the decreases listed above.

Key Social Media Mentions and Highlights

- @FBI, which has more than 2.1 million followers on Twitter, was highly engaged on the social platform throughout the month, tweeting weekly in October. Following is a snapshot of the FBI’s efforts:
  - On Oct. 3, @FBI promoted its blog, which featured an NCSA-created infographic and a resource for each weekly theme. The tweet has been retweeted more than 400 times and liked more than 500 times.
  - During Week 2, @FBI tweeted about protecting employees and businesses from work-related scams; the post has been retweeted more than 260 times and liked more than 300 times.
  - @FBI also tweeted during Week 4, aligning with the cybersecurity workforce theme by encouraging people to study STEM. The tweet has been retweeted more than 175 times and has more than 360 likes.

- The Small Business Administration (SBA) played a key role on social media during Week 2, promoting its small business training to its 480,000 Twitter followers and holding an #SBAChat Twitter chat on cybersecurity for small businesses in honor of the month. NCSA, STOP. THINK. CONNECT.™ and Michael participated in the chat, which had a potential reach of 2.6 million.

- Robert Herjavec, the “shark” on ABC’s Shark Tank and CEO of Herjavec Group, has been a loyal supporter of NCSAM on social media. In 2017, Robert tweeted in advance of the month and helped to drive engagement in Week 1’s record-breaking #ChatSTC Twitter chat.

- Girl Scouts of the USA joined in the conversation both on Capitol Hill and on Twitter to 77,000 followers, promoting the organization’s joint efforts with Palo Alto Networks in cybersecurity education and careers.

- A number of U.S. embassies joined the conversation, including Ghana (80,200 followers), Jakarta (344,000 followers), Madrid (30,800 followers), the Philippines (779,000 followers) and Uganda (123,000 followers). Many of the handles tweeted in their respective language(s) and made use of STOP. THINK. CONNECT.™ and NCSAM messaging and graphics.

- Ready.gov shared STOP. THINK. CONNECT.™-branded resources with its 141,000 followers towards the end of the month.

Key NCSAM Activities

Pre-October
- Utah Valley University (UVU) campaign:
  - UVU, in partnership with NCSA, conducted one of the first-ever cybersecurity saturation awareness campaigns for a targeted population (the campus community of 37,000+ students plus faculty and staff). The campaign was designed to understand what UVU students and faculty know about cybersecurity, what they are doing to be safe online and what they want to know about cybersecurity. As part of the initiative, UVU rolled out mandatory multi-factor authentication for faculty and optional...
Prior to NCSAM, a select group of students took a survey to determine their knowledge of cybersecurity and what gaps existed. Then, during October and November, a student PR class (with the help of NCSA and Thatcher+Co.) was tasked with campus outreach and publicity with the goal of getting students to implement two-factor authentication with the Duo app. The students created a campaign plan that included social media outreach, digital and paper signage, a campus information booth and distributed text messages via UVU platforms to promote the program.

- Countdown to NCSAM press release distributed nationally on Sept. 5:
  - The release encouraged everyone to get #CyberAware in October and share the responsibility of protecting the internet. In addition, a call to action for Champions and the weekly themes were prominently featured.

- Open letter to Congress sent on Sept. 14:
  - The letter was distributed to Senate and Hill staffers (both parties) and highlighted details on how to support NCSAM and easy ways to get involved and make a difference.

- Pre-NCSAM event for Capitol Hill staff on Sept. 14:
  - The event was sponsored by U.S. Rep. Jim Langevin (D-RI) and Rep. Mike McCaul (R-TX), co-chairs of the Congressional Cybersecurity Caucus. DHS representative Princess Young spoke about opportunities for NCSAM participation, and a panel discussion was held.

- NCSAM RMT on Sept. 26 in top U.S. markets:
  - NCSA and DHS conducted a very successful RMT during the morning drive time. A strong case was made for "why NCSAM"; weekly themes were highlighted and valuable resources shared. In total, there were 17 interviews, which reached 18 million+ listeners nationwide in several of the country's largest markets, including New York, Los Angeles, Philadelphia, San Francisco and Washington, D.C.

- International-focused announcement of NCSAM and Cyber Security Awareness Month (CSAM) distributed nationally and internationally on Sept. 27:
  - Digital citizens worldwide were reminded of the shared global responsibility to secure the internet. In addition, the global launch at OAS was showcased along with examples of international collaboration with various organizations. NCSA repurposed a NCSAM infographic with STOP. THINK. CONNECT.™-based tips and made it available for translation.

- On Sept. 30, President Trump proclaimed October as NCSAM:
  - The presidential proclamation encouraged consumers and all businesses to work together to improve the internet's safety and security. DHS' STOP. THINK. CONNECT.™ campaign was highlighted.

**October**

**Week 1: STOP. THINK. CONNECT.™: Simple Steps to Online Safety**

- News of the Week: Week 1 shared a variety of consumer-focused news, including the following: Raytheon’s “Shared Responsibility” stat; top consumer cyber concerns; ITRC’s Aftermath Survey; Home Instead Seniors Survey and ESET’s Cybersecurity Cash Car.

- Launch Event: The official U.S. launch of NCSAM 2017 – hosted by OAS in partnership with NCSA, DHS and the State Department – took place on Oct. 3 at the Hall of the Americas in Washington, D.C. The event convened high-level speakers and cybersecurity experts from a variety of nations and backgrounds. Content was extremely well received and focused on online security from an international perspective.
perspective, and how to best work together on cybersecurity issues today and in the future. The event kicked off with a Twitter chat, and there was strong social engagement throughout the day. DHS Assistant Secretary Manfra delivered opening remarks, and a series of engaging panel discussions followed. More than 150 guests attended in person, and 1,314 joined in via livestream, with an average watch time of 41 minutes.

Additional Event: NCSA was invited to facilitate the CyberSecure My Business workshop for the FS-ISAC Fall Summit guests on Oct. 2 in Baltimore. More than 60 banking executives attended and feedback was positive. In addition, FS-ISAC indicated their desire to grow their relationship with NCSA following the workshop.

• Week 2: Cybersecurity in the Workplace Is Everyone’s Business
  News of the Week: Reminding everyone of the critical role that each employee – from the breakroom to the board room – plays in a cybersecure workplace was Week 2’s theme. In addition, NCSA announced the launch of its new CyberSecure My Business™ webinar series, showcased new MediaPro research and addressed top cyber concerns for business.

NCSA/DHS Event: On Oct. 10, the National Rural Electric Cooperative Association (NRECA) – a membership organization of 900+ consumer-owned electric utilities – held a SMB-focused event and workshop in Arlington, VA. Federal Trade Commission Acting Chairman Maureen Ohlhausen delivered the keynote address, and DHS’ Chris Butera and representatives from NRECA and the U.S. Department of Energy participated in a panel discussion moderated by Michael Kaiser. Close to 100 guests were present, and more than 1,700 have since viewed the livestream. Later that morning, NCSA’s Kristin Judge conducted a hands-on SMB-focused workshop, which 100% percent of post-event survey respondents indicated they would recommend.

Additional Events: NCSA’s CyberSecure My Business™ webinar series launched on Oct. 10. Content addressed the issues of ransomware and phishing. Experts from the public and private sectors addressed how to help SMBs better understand how to combat these common attacks. More than 500 individuals joined the webinar.

In Washington, D.C., on Oct. 14, the FIDO Alliance, NCSA and the Electronic Transactions Association hosted the Future of Authentication Policy Forum to discuss the critical importance of strong, multi-factor authentication.

• Week 3: Today’s Predictions for Tomorrow’s Internet
  News of the Week: IoT was the hot topic for Week 3 in addition to the NCSA and Nasdaq Cybersecurity Summit.


NCSA/DHS Event: On Oct. 16, NCSA partnered with Nasdaq to host “Securing Breakthrough Technologies – The Next Five Years, a NCSA and Nasdaq Cybersecurity Summit” at the Nasdaq MarketSite in New York City’s Times Square. This event brought together experts from industry, government and academia to discuss cutting-edge innovations in artificial intelligence, the IoT, machine learning, authentication and standards and what they mean for the average person, and how we interact with technology. With more than 100 guests in attendance along with 17 media and more than 12,000 livestream views, the event’s timely panel discussions and TED-style talks were well received. The daylong event concluded with DHS Assistant Secretary Manfra ringing of the Nasdaq Closing Bell in honor of NCSAM.
• **Week 4: The Internet Wants You: Consider a Career in Cybersecurity**

**News of the Week:** Raytheon and Forcepoint in partnership with NCSA released the fifth annual “Securing Our Future; Cybersecurity and the Millennial Workforce” study. In addition, Facebook showcased its commitment to careers in cybersecurity, with a focus on diversity.

**Virtual Events:** NCSA hosted a series of timely livestream interviews addressing careers in cybersecurity from a breadth of perspectives. Over the period of several days, seven discussions were shared via livestream, reaching more than 6,720 views. The following highlights the speakers and their areas of expertise:

- Rodney Petersen, National Initiative for Cybersecurity Education (NICE): Workforce/Education
- Michael Kaiser, NCSA: Raytheon Study Results
- Elena Steinke, Women’s Society of Cyberjutsu: Getting Women into Cyber
- Kerry-Ann Barrett and Mariana Cardona, OAS: OAS’ Program to Engage Students in Cybersecurity
- Nicole Dean, Accenture: Personal Path into Cybersecurity, Inspiring a New Workforce
- Sarah Geoffory, AT&T: Personal Path into Cybersecurity, A Day at Work
- Princess Young, DHS: Personal Path into Cybersecurity, DHS’ Cyber Workforce Efforts

**Social Collateral/Weekly Materials**

NCSA developed a breadth of materials for NCSAM Champions, partners and visitors to staysafeonline.org to use and share on social media, on their websites and with friends, family, colleagues and the community. NCSA has established a strong distribution base and sent this collateral via a weekly email to its mailing list. Each email shared the coming week’s infographic(s) (see below), social media content, noteworthy partner resources and event details – creating a one-stop shop for promoting NCSAM’s news and ongoing efforts. This information was very well received and provided easy access for individuals and organizations alike to participate in the month.

NCSA worked with DHS and partners - including Microsoft and Raytheon - to create the following series of compelling infographics, which were shared on NCSA's website and via both traditional and social media.
Stakeholder Engagement
NCSAM 2017's far-reaching awareness was due in part to the variety of activities executed by numerous stakeholder groups, which included academic institutions, federal, state and local government entities and private companies. The following is a snapshot of different organizations’ commitment to the month. NCSA tried to gather as many examples as possible during a tight timeframe for reporting in 2017.

DHS Participation in NCSAM
Note: The following details regarding DHS involvement and federal, state and local government NCSAM support were shared with NCSA by Princess Young.

DHS Activity Highlights

• The DHS STOP. THINK. CONNECT.™ campaign partner program reached 444 total partners, growing by 6 percent during October with the addition of 21 new partners.

• DHS distributed a weekly newsletter to its Friends program – individuals who have signed up to support the campaign. The newsletter reached over 41,000 individuals.

• DHS coordinated three keystone events which generated in-person attendance of 370+ and more than 15,000 digital viewings.

• DHS distributed a weekly email message to its STOP. THINK. CONNECT.™ partners with tips and resources aligning to each week’s theme.

• DHS published several blog posts aligning with the weekly themes (DHS blog and DHS STC blog).

• DHS participated in the five weekly Twitter chats hosted by NCSA.

• The DHS.gov home page promoted NCSAM with an image on its rotating banner.

• DHS promoted NCSAM internally to employees through leadership messages, a weekly Cyber Tips article in an employee newsletter and encouraging employees to take a selfie in the mobile #CyberAware selfie booth.

DHS Leadership Participation

• DHS participated in 17 interviews as part of the NCSAM radio media tour. DHS representatives included:
  o Jeanette Manfra, Assistant Secretary for Cybersecurity & Communications (CS&C)
  o Jeff Eisensmith, Chief Information Security Officer
  o Ben Scribner, CS&C/Cybersecurity Education & Awareness
  o Princess Young, CS&C/Cybersecurity Education & Awareness

• DHS participated in the Global Launch of Cyber Security Awareness Month hosted by the Organization of American States. DHS representation is below:
  o Jeanette Manfra provided welcome remarks.
  o Brad Nix from the United States Computer Emergency Readiness Team (US-CERT) participated on a panel, Working Together Globally.
Tom McDermott, DHS deputy assistant secretary for cyber policy, participated on a panel, *A Look Toward the Future*.

Omar Cruz from DHS US-CERT gave a Facebook Live interview, which garnered over 450 views.

DHS participated in the National Rural Electric Cooperative Association (NRECA) event *Insights on Cybersecurity for Electric Utilities* on Oct. 10. The event live stream was viewed more than 1,700 times. DHS representation included the following:

- Sabra Horne, director for stakeholder engagement and cyber infrastructure resilience, delivered opening remarks.
- Chris Butera from the National Cybersecurity and Communications Integration Center participated in a fireside chat about cybersecurity and the energy sector.
- Reggie McKinney, director of the Critical Infrastructure Cybersecurity Community Voluntary Program (C3VP), gave an overview of DHS resources for small and medium-sized businesses.

DHS participated in the NCSA/Nasdaq Cybersecurity Summit and the Nasdaq Closing Bell Ceremony.

- Jeanette Manfra participated in a fireside chat and formally closed the Nasdaq market on Oct. 16. She also participated in a Facebook Live interview with Nasdaq and NCSA that was viewed more than 1,200 times.
- Jeff Eisensmith participated on a panel, *Can the Internet of Insecure Things be Saved?*

DHS was part of a series of Facebook Live interviews discussing cybersecurity careers, the NCSAM Week 4 theme.

- Princess Young talked about her own experience transitioning to the cybersecurity field as an alumna of the CyberCorps® Scholarship for Service program. Her Facebook Live interview was viewed more than 750 times.

**Federal Government Select Activities**
Twenty-one federal agencies reported their NCSAM activities to the STOP. THINK. CONNECT.™ campaign. Highlights of these activities are listed below:

- The U.S. National Security Administration (NSA) supported NCSAM through social media posts, email messages, website content, NSA.gov articles and blogs. NSA also participated in/or hosted 15 major activities and presentations, including career fairs, a cybersecurity summit, 2 Cyber Rocks concerts with informational tables for the NSA and CIA and panel discussions.

- The Department of State (DoS) focused its NCSAM 2017 efforts on sharing digital resources including fact sheets, weekly communications, videos and daily reminders. Additionally, DoS offered online and in-person cybersecurity training courses relevant to DHS’s five NCSAM themes highlighted throughout the month, including a special town hall webinar for Information System Security Officers to discuss
cybersecurity innovation at the Department. Overall, DoS provided more activities than in any year past and experienced a huge surge in hits to its website (with a 70% increase in visits to its NCSAM website over 2016).

- The U.S. Department of Health and Human Services (HHS) held five separate events that included presentations by subject matter experts (SMEs) like the chief information security officer (CISO) and deputy CISO, the director of workforce planning and representatives from both the cybersecurity learning team and the risk management team. These events had a combined total of 1,108 attendees.

- The U.S. Postal Service (USPS) launched a NCSAM-themed awareness campaign to 600,000+ employees, including creating a series of articles, electronic screensavers, one-pagers, posters, and other artifacts, supplemented by a national call with key stakeholders and talking points for USPS leadership to share with employees. Additionally, the USPS CISO office uploaded NCSAM-themed website content across three CyberSafe at USPS websites, including promotional banners, educational one-pagers and a video to provide easy access to cybersecurity tips, tricks and best practices. Lastly, USPS hosted its 2017 USPS Cybersecurity Awareness Fair in recognition of NCSAM. The fair was attended by nearly 400 USPS employees.

Select State, Local, Tribal and Territorial Government Activities

- Forty-seven states, 90 localities and one territory (Puerto Rico) signed proclamations declaring October as NCSAM (as reported to the Multi-State Information Sharing and Analysis Center).

- Stearns County, MN, hosted a NCSAM STEM/SPARK project, which invited high school students to discuss cybersecurity careers. The county also posted weekly NCSAM materials on its internal employee intranet using the weekly messages and materials provided by the campaign, reaching 900 local government employees.

- The City of Virginia Beach, VA, provided cybersecurity information, including the DHS Cyber Security for Older Americans and the Mobile Use tip sheets, to more than 300 senior citizens in the community at the Mayor’s Commission on Aging Senior Showcase. The city also built a website (www.vbgov.com/PracticeSafeCyber) to feature cybersecurity tips and information and interactive tools such as a password strength checker and an employee cybersecurity workplace quiz. In addition, the city promoted NCSAM through social media (28,700 Facebook and 66,900 Twitter followers) and website content related to the themes.

- The State of South Dakota shared social media posts, email messages, newsletters and blogs throughout the month. Additionally, the state developed cybersecurity splash pages to appear when users opened their internet browsers and distributed cybersecurity posters and calendars to K-12 schools during scheduled visits. The state’s efforts reached about 8,000 state users.

NCSA’s Board of Directors, Partner Organizations and Champions

Note: The following content was submitted directly to NCSA for inclusion in this report.

NCSA Board Member Companies

ADP

ADP carried out both a digital and physical campaign in many of its facilities across the globe. ADP chose four themes for communications through the month (one each week), which addressed hot security topics (e.g., email security, travel safety, passwords, social engineering) and were relatable to most employees. In ADP communications, tips, fun graphics and memes were shared to help engage employees. The goal was to promote security awareness at work and in employees’ personal lives. The following is a list of employee-focused initiatives:

- Clean Desk Checks: Leaving funny notes on employees’ desks
- Security Hot Topic Sessions: In-person sessions and webcasts
• Security Fair: Staffed tables set up with activities or information
• Brochure Display: Tables set up in various central locations with “take away” security awareness materials
• Security Awareness Quiz Challenge: Four digital quizzes were published each week, and if employees completed all of them by the month’s end, they were entered into a random drawing to win an Amazon Echo
• Communications: ADP had multiple portal articles and banners, posters and internal social media promotions during the month to keep employee engagement high

Cisco
During NCSAM, Cisco took the opportunity to raise awareness around critical industry issues and threats to businesses and consumers. In a total of 27 stories, Cisco executives discussed the need for organizations to cultivate a culture of cybersecurity and the industry’s need to come together to address the information security talent shortage – empowering aspiring talent to pursue careers in cybersecurity.

Cisco partnered with NCSA to participate in three Twitter chats, engaging social media users and addressing prime security concerns and questions. Cisco’s John Stewart, senior vice president and chief security trust officer, joined Michael Kaiser, NCSA’s executive director, for a podcast discussion on tomorrow’s emerging threats and how businesses need to prepare for them. In addition, Cisco’s Anthony Grieco, trust strategy officer and senior director, partnered with Michael to raise awareness on Internet of Things (IoT) security and the importance of establishing baseline requirements in a Q&A appearing in the Huffington Post.

The conversation and actions transcended platforms, with Cisco SMEs participating in webinars that addressed topics such as GDPR and careers in cybersecurity and contributing to Cisco’s security blog with multiple weekly posts throughout October.

The team’s efforts continued by participating in two panel discussions at the NCSA and Nasdaq Cybersecurity Summit in New York, with Cisco addressing the role of IoT security amid today’s digital transformation as well as the emergence of artificial intelligence (AI) in cybersecurity. Anthony Grieco represented and elevated Cisco’s awareness efforts in Europe with his participation in the ENISA European Cyber Security Month Kick-Off Event in Tallinn, Estonia. Later in the month, he delivered the keynote at the NIAS2017, NATO’s annual cyber symposium, in Mons, Belgium.

ESET
ESET created a NCSAM campaign with a goal of generating broadcast media coverage, engaging and educating the public while providing a unique way to give back to NCSA. This was the rationale for the Cybersecurity Cash Car, which gamified cyber awareness and education. Eight wrapped ESET and NCSAM vehicles were deployed on the streets of San Diego – to act as mobile billboards, sporting an ESET.com/cybersecurity URL – a #CyberAware page that contained free cyber resources, including ESET
Cybersecurity Awareness Training, a free malware scanner and information about the Cash Car game. One of those vehicles was the designated “Cybersecurity Cash Car,” which would pop up and park in locations around San Diego with the ESET #CyberAware team giving cash to people who answered cyber quiz questions correctly.

On average, each participating player won $60 in the one minute they had to answer questions, and ESET matched players’ winnings with a donation to NCSA. Local broadcast media covered the pop-up Cybersecurity Cash Car on multiple days (CBS 8 featured the car twice, and NBC 7 did as well, with a collective viewership of more than 100,000). Over 300 visited the #CyberAware page (from noticing the hashtag on the Cash Car), and the mobile billboard (the wrapped cars) generated more than 14 million impressions during October. The campaign ended with ESET gifting NCSA with $2,000, which matched the cash won while playing the game.

Wells Fargo
NCSAM is an opportunity for Wells Fargo. Chief Information Security Officer (CISO) Rich Baich is the company’s primary spokesperson on cybersecurity topics and has built his credibility with team members, customers, industry associations and the media through multiple internal and external communications.

Activities
Audience: Team Members
- Teamworks articles featuring quotes from Rich and other leaders
  - Staying a step ahead of cyberthreats (Oct. 2) features a video of Rich discussing current cybersecurity threats
  - With biometrics, you are the password (Oct. 19) (also on Wells Fargo Stories) resulted in 55 comments as of Oct. 26
  - Information security is every team member’s business supports an enterprise information security (EIS) policy goal, driven by the E&A team
  - Evolution of cybersecurity article (Oct. 30), which features an industry video Rich was involved in producing and hosted by NCSA
- Cloud Security Virtual Summit – four-hour virtual conference on important and newly developing issues for 200 attendees
- Sent NCSAM message on Oct. 26 to EIS, posted on CR portal

Audience: Customers
- Wholesale marketing website landing page with video, articles and information attributed to Rich used with Wells Fargo’s NCSAM campaign

Audience: Industry
- New membership to NCSA
- Cybersecurity video co-written by Wells Fargo, hosted by NCSA

Audience: Media
- The Banker, “How banks are combating the cyber threat,” Oct. 2
- SC Media, “Artificial intelligence and machine learning needed to backstop humans,” Oct. 16
- Additional stories
  - Wall Street Journal CIO Journal article on security automation
  - Banking Strategies article on AI and cybersecurity
  - Forbes.com article on information security intersection between business and education
Rich participated in two panel discussions at the Oct.16 NCSA event “Securing Breakthrough Technologies: The Next Five Years” and participated in the Nasdaq closing bell ceremony.

Supporting NCSA media efforts in support of cyber video launch.

**NCSA’s Trusted Partners**

**Arm**

Arm technology is at the heart of the computing and connectivity revolution that is transforming how people live and businesses operate. The company’s advanced, energy-efficient processor designs are enabling the intelligence in 100 billion silicon chips and securely powering products from the sensor to the smartphone to the supercomputer. With more than 1,000 technology partners, including the world's largest business and consumer brands, we are driving innovation into all areas from the chip to network and the cloud. Arm was a NCSAM 2017 Champion.

Arm launched its Security Manifesto and Platform Security Architecture at Arm TechCon at the end of October and also participated in two Twitter chats.

**Council of Better Business Bureaus (CBBB)**

CBBB supported NCSAM through a variety of programs.

**Reports and Support Initiatives:**


**Social Media:** Participated in five Twitter chats

- Oct. 3 Twitter Chat + Living Twitting during launch event: 7.2K impressions
- Oct. 5 Twitter Chat: 4.4K impressions
- Oct. 12 Twitter Chat: 3.6K impressions
- Oct. 19 Twitter Chat: 3.7K impressions
- Oct. 26 Twitter Chat: 4.0K impressions

**5 Facts About Cybersecurity Series** – released every Monday as part of the CBBB’s social campaign for the Cybersecurity Awareness Month activities. The facts were used to drive engagement.

Total: 53,805 impressions

**Events:** Early this summer, Better Business Bureau (BBB) Chicago and Northern Illinois launched a panel series to alert and educate the Chicago and Northern Illinois business communities about the surging peril of cybercrime in business. The BBB moderator and two experts from cybercrime-related accredited companies have presented five times, including three panels hosted by the City of Chicago at the business community meeting room at City Hall. The BBB is offering a free panel to speak to any business group of 30 or more, and speakers from the BBB who have been trained in the presentation have talked to variety of groups. In addition, CBBB’s Bill Fanelli presented 5 Steps to Better Business Cybersecurity at the McAfee Conference in Las Vegas, NV; approximately 70 people were in attendance for this presentation.

**EDUCAUSE**

EDUCAUSE is a nonprofit higher education technology association and the largest community of IT leaders and professionals committed to advancing higher education. EDUCAUSE registered as a NCSAM 2017 Champion. It was EDUCAUSE’s 14th year supporting NCSA and NCSAM in higher ed. Here is a list of key accomplishments:

- 206 higher education institutions showed their support as official Champions (an increase from 173 in 2016).
• Over 130 attendees joined the Oct. 23 EDUCAUSE Live! webinar with guest speaker Jason Hoenich (Founder, Habitu8), who discussed “Shifting to Security Awareness 2.0.” NCSA Executive Director Michael Kaiser helped kick off this NCSAM online event.
• Throughout the month of October, EDUCAUSE published a series of posts focusing on faculty and student perceptions of information security (from the results of a 2017 research report). These publications appeared in the EDUCAUSE Review Data Bytes, Security Matters and Transforming Higher Education columns.
• The Higher Education Information Security Council (HEISC) and several members of the EDUCAUSE community participated in the #ChatSTC Twitter chats in October and November.
• EDUCAUSE supports security awareness in higher education with the year-round Campus Security Awareness Campaign, a framework that assists information security professionals and IT communicators as they develop or enhance their security awareness plans. Monthly topic features in the EDUCAUSE Review Security Matters column include ready-made web and social media content that makes it easier to keep a steady stream of security and privacy best practices prominent in campus communications. The 2018 content is now available for anyone preparing next year’s awareness and education efforts.

European Union Agency for Network and Information Security (ENISA)
This was the fifth consecutive awareness campaign put together by the EU Cybersecurity Agency ENISA, the EU Commission's DG CONNECT and their partners. Similar to last year, ENISA also partnered with Europol's European Cybercrime Centre (EC3) to promote cybersecurity awareness and education. During the month of October, approximately 530 activities – such as conferences, workshops, seminars and online courses – took place throughout Europe. There was an increase of more than 15% of activities in comparison to European Cyber Security Month (ECSM) from the previous year. All of the initiatives during the month were designed to help make the internet a safer place for everyone.

The ECSM keystone event was held under the Estonian Presidency at Tallinn University of Technology at the end of September. The event was co-organized by ENISA and the Estonian Information Systems Authority. Panel discussions centered on the themes of the month and the role of awareness raising within each of the topics. The group of panelists included esteemed cybersecurity experts from Intel, Hytrust and APWG, as well as members of NCSA's Board of Directors, including William O'Connell from ADP and Anthony Grieco from Cisco.

This year's ECSM campaign highlighted the following themes:
• Week 1: Cybersecurity in the workplace – cyber-hygiene practices for subject matter experts
• Week 2: Governance, Privacy & Data Protection – preparation for EU’s General Data Protection Regulation
• Week 3: Cybersecurity in the home – threats related to IoT
• Week 4: Skills in cybersecurity – educating and growing the cybersecurity workforce

Although ECSM 2017 has ended, the need for cybersecurity awareness continues. ECSM works continuously to promote a safer, more secure and more trusted internet. Visit cybersecuritymonth.eu to learn more about how to protect yourself online.

Fannie Mae
Fannie Mae serves the people who house America and is a leading source of financing for mortgage lenders, providing access to affordable mortgage financing in all markets at all times. This year, the Fannie Mae team opted to switch things up a bit. Last year, the information security team hosted a one-day event, which consisted of breakout sessions, guest speakers and an all-employee expo. For 2017, the initiatives were split up throughout the entire month of October. Fannie Mae hosted guest speakers (Secret Service & FireEye) and even looped in some of the vendors with whom it works (Visium & FireEye) to help keep the organization safe. The following presents highlights of NCSAM 2017 accomplishments/initiatives:
• Week 1: Message out to the entire organization from Fannie Mae’s CISO – Oct. 4
• Week 2: Brown Bag – Access Management (256 attendees in total) – Oct. 12
• Week 3: Brown Bag – AppSec/nVisium (295 attendees in total) – Oct. 18 and Brown Bag Risk, Governance & Awareness (95 attendees in total) - Oct. 19
• Week 4: Speaker Symposium (402 attendees in total) – Oct. 24; InfoSec/Privacy YammerCast (197 attendees in total) – Oct. 25
• 2017 Information Security Expo (141 attendees in total) – Oct. 26
Herjavec Group
Founded in 2003 by dynamic IT entrepreneur Robert Herjavec, Herjavec Group supports the IT security lifecycles of businesses and their infrastructures. The company provides various cybersecurity solutions such as payment card industry audits, social engineering and vulnerability assessments and managed security services. This October, Herjavec Group participated in the following ways:

- Partnered with Cybersecurity Ventures to produce and release the 2017 Cybercrime Report during NCSAM.
- Launched its first podcast episode specifically for NCSAM, interviewing several Herjavec Group team members; the podcast got a lot of social media traction.
- Published four pieces of original content, including “Tips for Getting a Job in Cybersecurity,” “How Businesses can Avoid Phishing Scams,” “How to Stay Safe Online” and “How to Raise a Cyber Savvy Kid in a Cyber World.”
- Produced a video featuring tips for staying safe online.

Healthcare Information and Management Systems Society (HIMSS)
HIMSS North America, a business unit within HIMSS, positively transforms health and healthcare through the best use of information and technology throughout the United States and Canada. HIMSS was a NCSAM 2017 Champion and supported the month by:

- Publishing a tip sheet with practical tips for small physician practices, available for download at www.himss.org/ncsam.
- Actively participating in all NCSAM Twitter Chats hosted by Stay Safe Online with HIMSS staff and members of the HIMSS Privacy and Security Committee.

Identity Theft Resource Center (ITRC)
The ITRC is a nonprofit organization established to support victims of identity theft in resolving their cases and broaden public education and awareness in the understanding of identity theft, data breaches, cybersecurity, scams/fraud and privacy issues. ITRC was a NCSAM 2017 Champion. The following shares a summary of ITRC’s support of October:

- Child identity theft op-ed with NCSA: http://www.huffingtonpost.com/entry/qa-with-eva-velasquez-of-the-identity-theft-resource_us_59d253c5e4b0f58902e5ce10
- #ChatSTC participant
- Daily share of NCSA #CyberAware materials
- NCSAM feature in ITRC TMI weekly newsletter
- ITRC blogs curated for NCSAM:
MediaPro
MediaPro, headquartered in Bothell, WA, works with many Fortune 500 companies and mid-sized businesses to reduce human risk in cybersecurity, privacy and compliance by delivering comprehensive employee awareness programs. MediaPro was a NCSAM 2017 Champion. The following summarizes several of MediaPro’s key accomplishments:

• Released its second annual State of Privacy and Security Awareness Report, which was featured in the Week 2 NCSAM press release and a handful of tech/cybersecurity news outlets, such as Dark Reading. Overall, 175 people downloaded the full report in October, while 276 people viewed the web page hosting the report infographic.
  o Full report page (and access to take the survey the report is based on): https://pages.mediapro.com/2017-State-of-Privacy-Security-Awareness.html

• Hosted two NCSAM webinars – one focusing on the above-mentioned report and the other presenting a hypothetical year in the life of a security awareness program manager. This second webinar presented advice on how someone responsible for security awareness at a given company could develop a comprehensive security awareness program. A total of 205 people registered for both webinars.
  o A Year in The Life of A Security Awareness Program Manager: https://pages.mediapro.com/AYearInTheLifeOfASecurityAwarenessManager_RegistrationLandingPage.html

• Launched its second annual series of NCSAM “toolkits,” which are collections of both MediaPro-sourced and STOP. THINK. CONNECT.™ downloaded resources. Each of the five toolkits was aligned with each of the five NCSAM weekly themes. A total of 211 people opted in to get all five toolkits.

• Debuted its first-ever Awareness Program Excellence Awards, recognizing exemplary awareness program initiatives. Eleven organizations submitted, and five were recognized with awards.
  o Award Press Release: https://www.mediapro.com/blog/winners-mediapro-awareness-program-excellence-awards/

• Introduced its “Cybersecurity Pledge” initiative, designed to be taken by employees and shared socially.
  o Pledge page: https://www.mediapro.com/blog/mediapro-cybersecurity-pledge/

Public Safety Canada
Public Safety Canada’s Get Cyber Safe is a national public awareness campaign created to educate Canadians about internet security and the simple steps they can take to protect themselves online. The campaign’s goal is to bring together all levels of government, the public and private sectors and the international community to help Canadians be safer online. Public Safety Canada adapts NCSAM themes to Canadian audiences and promotes shared messaging via the Get Cyber Safe campaign. The Canadian Cyber Security Awareness Month (CSAM) 2017 themes were as follows (in English and French):

• Week 1 (Oct. 2-6): Get Cyber Safe and STOP. THINK. CONNECT.™: Simple Steps to Online Safety
  Semaine 1 du 2 au 6 octobre : Pensez cybersécurité et ARRÊTEZ. RÉFLECHISSEZ. BRANCHEZ-VOUS.MC : Mesures simples liées à la sécurité en ligne

• Week 2 (Oct. 9-13): Cyber security in the Workplace is Everyone’s Business
  Semaine 2 du 9 au 13 octobre : La cybersécurité en milieu de travail concerne tout le monde

• Week 3 (Oct. 16-20): Privacy Protection and the Internet of Things
The following shares a summary of Public Safety Canada’s support:

- Participated in three of the STOP.THINK.CONNECT.™ CSAM Twitter chats.
- Wrote four blog posts in support of each of the four CSAM themes.
- Guest blog post by Canadian Bankers’ Association featured on GetCyberSafe.ca blog.
- GetCyberSafe guest blog post featured on Telus WISE site (WISE Internet and Smartphone Education).
- CSAM and GetCyberSafe featured in CSE’s Cyber Journal, (Edition 12), a newsletter for stakeholders and Canadian organizations with a focus on current and emerging technologies:
  - CSAM messages featured on Digital Display Networks of Canada Post and Service Canada service centres.
  - Print articles in community newspapers across Canada (generated more than 2 million impressions).
  - Content shared and posted by other federal government departments and agencies such as Canadian Radio-television and Communications, Innovation Science and Economic Development (Your Money Matters campaign), Royal Canadian Mounted Police and
  - Created a CSAM social media post for each theme (one per week on Facebook, Twitter and LinkedIn)

**Retail Cyber Intelligence Sharing Center (R-CISC)**
The Retail Cyber Intelligence Sharing Center (R-CISC) is the trusted cybersecurity resource for the retail industry and consumer product and service organizations and cybersecurity industry partners worldwide. The R-CISC, through its operation as the Retail ISAC, supports its member base that represents over $1 trillion in annual revenues by serving as the conduit for collaboration, threat intelligence sharing and cooperation. R-CISC does this by building and sustaining valuable programs, partnerships, products and opportunities that enable their members to grow in their trust-based relationships, strategic knowledge and tactical capabilities. Through the R-CISC, members of all sizes share cyber intelligence on incidents, threats, vulnerabilities and associated threat remediation. R-CISC does this because as a community, they understand that they are stronger together. R-CISC was a NCSAM 2017 Champion. The following presents a list of R-CISC accomplishments:

- R-CISC hosted Cyber Intelligence Summit in October (#securingretail002 & #cyberaware), [LINK](#), [LINK](#), [LINK](#)
- R-CISC worked with other information sharing and analysis centers (ISACs), the FBI, the U.S. Secret Service (USSS) and Symantec Collaborate to Fight Business Email Compromise hosting workshops nationwide during October, November and December, [LINK](#)
- Two R-CISC Members Offer Space for USSS/FBI BEC Workshops, [LINK](#)
- R-CISC hosted first annual The Importance of Women in Cyber Panel, [LINK](#)
- R-CISC hosted a webinar, ThreatQ And MGM Resorts International Discuss Threat Intelligence Operations And Management, [LINK](#)
- R-CISC hosted a webinar, Cross-industry Collaboration For More Effective Fraud Prevention with LexisNexis, [LINK](#)
• R-CISC hosted a webinar on overcoming legal barriers to information sharing, [LINK]
• R-CISC hosted an associate member webinar, How to Use Automated Feeds with Anomali, [LINK]
• R-CISC hosted Cyber Peer Choice Awards, [LINK, LINK]
• R-CISC’s executive director was a panelist at the ISAO Standards Organization in Washington, D.C. Panel: “How to Launch a Cross-Sector Intelligence Exchange,” [LINK]
• R-CISC’s executive director was a panelist at Global Gaming Expo on actionable intelligence: efficient and effective security solutions, [LINK]
• Cyber Secret Weapon story, [LINK]
• Best practices for sharing intel story, [LINK]
• Hosted Q&A discussions with members around importance of cybersecurity for #CyberAware Month, [LINK]
• Countless #CyberAware social media posts, https://twitter.com/RetailCISC
• In support of NCSAM, hosted the webinar Retail Holiday Threats, Trends, & Mitigation Strategies With Booz Allen Hamilton, [LINK]
• R-CISC weekly holiday calls for members, [LINK]

Underwriters Laboratories (UL)
UL, a safety science company, has developed a security certification based on a series of standards for IoT products to help mitigate the safety and performance risks of connected technologies. UL mitigates cybersecurity risks by assessing software weaknesses, minimizing exploitation, addressing known malware, reviewing security controls and increasing security awareness. UL enables manufacturers to continue their innovations while producing more secure products and systems, bringing end users increased confidence in the products and systems that they use. Please see below for UL’s accomplishments and social media posts:

• Huffington Post Q&A on securing critical infrastructure with NCSA Executive Director Michael Kaiser and UL’s cybersecurity lead, Ken Modeste: Q&A with Ken Modeste of UL: Securing Our Critical Infrastructure (published Oct. 30)
• UL’s Ken Modeste served as a panelist for the NCSA/RSA Conference webinar on IoT security (took place Oct. 19)
• UL participated in the Week 2 Twitter chat “Cybersecurity in the Workplace is Everybody’s Business” (took place Oct. 12)
• UL participated in the Week 5 Twitter chat “Securing Critical Infrastructure” (took place Nov. 1)
• UL drafted a blog post that was included on the NCSA’s blog, End-to-End Cybersecurity for Critical Infrastructure – from IIoT to Electronic Physical Security (posted on NCSA’s blog on Oct. 30)
• Social posts from @ULCommercial
  - https://twitter.com/UL_Commercial/status/925750778463125504
  - https://twitter.com/STOPTHNKCONNECT/status/925791555759128577 (retweet)

U.S. Department of State
The Department of State is the United States’ federal executive department that advises the president and leads the country on foreign policy issues. The department's mission is to shape and sustain a peaceful, prosperous, just and democratic world and foster conditions for stability and progress for the benefit of the American people and people everywhere. Its NCSAM activities included:

• Incorporating a digital activity and communication every weekday throughout the month to raise awareness about the importance of cybersecurity. These activities aligned with the five NCSAM themes issued by DHS and included daily computer pop-up reminders, tips about cybersecurity and posts on the department’s internal social media platform using #CyberAware.
• Offering online and in-person cybersecurity training; courses relevant to DHS’ five NCSAM themes were highlighted throughout the month, including a special town hall webinar for information system security officers to discuss cybersecurity innovation at the Department. Additionally, a briefing and talking points were provided to all cybersecurity officers and managers at embassies across the world and domestically to present to their staff about NCSAM.
• Creating a website dedicated to NCSAM that included a list of activities, videos, training and links to additional information and resources.
• Developing two videos, including an important message from the department’s cyber directorate assistant director and an animated video to show the significance of NCSAM and how to stay safe online.

NCSAM Champions

American Family Insurance (AmFam)

AmFam is a fortune 500 company focusing on property, casualty and auto insurance headquartered in Madison, WI, with approximately 22,000 employees across the enterprise. The company’s NCSAM activities included:

• Hosting guest speaker special agent Byron Franz of the FBI, whose presentation from AmFam’s auditorium was broadcasted live to all of the company’s satellite locations. He offered tips on a variety of cybersecurity topics, including best practices for home and work.
• Arriving early to give employees a Halloween greeting as they got to work with candy, security swag and advice.
• Holding an all-day open house in the IT security department. Tables were filled with goodies, and staff spoke to anyone who stopped by about what the security teams do to keep AmFam safe and what their different roles entail.Aligning with NCSAM Week 4’s cybersecurity workforce theme, staff spoke in detail about careers in the field.
• Creating fun supporting posters that spoofed lyrics to popular songs with online safety tips.

Attivo Networks®

Attivo Networks provides deception technology for real-time detection, analysis and accelerated response to today’s advanced cyberattacks. During NCSAM, the company promoted safer security practices with the following initiatives:

• Attivo hosted a capture the flag event at ISSA International as a fun, interactive way to educate attendees about cybersecurity and test information security skills with the added challenge of deception traps.
• Attivo CEO Tushar Kothari posted #CyberAware tips every Tuesday and Thursday on Twitter. The #TushnarTips outlined common security concerns related to protecting everything from an organization’s network to IoT devices and more.
• The company blogged about NCSAM, shared Halloween-themed security practices and explained how deception-based defenses can efficiently detect security threats and protect private information.

Center for Internet Security (CIS)

CIS is a forward-thinking, nonprofit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. The company’s CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response and recovery for U.S. state, local, tribal and territorial government entities. CIS’ efforts for October 2017 included:

• Kicking off the month with a NCSAM blog and infographic that highlighted the weekly themes; CIS followed up by posting weekly blogs that discussed timely topics such as “Want to Evade Cyber Criminals? Use These Three Tactics,”
Developing a Culture of Cybersecurity with the CIS Controls,” “Smart Devices, Smart Users – How to Stay Secure in an IoT World” and “Pursuing a Career in Cybersecurity? Three Tips from an Industry Veteran”.

- Announcing a multidisciplinary partnership with the University of Maryland School of Public Policy (SPP) for cybersecurity research. Through the partnership, CIS and SPP will pursue joint research initiatives, share specialized facilities and equipment, create opportunities for student engagement and more.
- Publishing a YouTube playlist on the 20 CIS Controls – a prioritized set of actions that can help protect an organization and its data from known cyberattack vectors.
- Creating graphics featuring CIS employees who shared cybersecurity tips for Week 1 and Week 2.

The Critical Thinking Child LLC
The Critical Thinking Child LLC empowers parents with innovative tools and educational resources needed to foster students’ academic achievement and build healthy cyber safety habits. Throughout October, the organization:

- Held educational sessions for parents and children (ages 3 to 13) on cyber safety tips and strategies.
- Partnered with local news media on a segment to raise awareness of frightening trends in cyberbullying and online predators.
- Facilitated group discussion to give preschool parents an opportunity to talk to other parents about cyber safety challenges in their homes and share ideas.
- Launched Cyber City, a children's book series containing spectacular storybook tales and adventures that promote online safety for kids ages 3 and up.

Def-Logix, Inc.
Def-Logix, Inc. is a team of cybersecurity experts with extensive background as government contractors. Def-Logix participated in NCSAM in the following ways:

- Hosted a Hack-Or-Treat commercial launch event for its new product. The gathering included a costume contest, food, drinks and a giveaway of the new system for the lucky winner.
- Created social media and web content such as articles, blog posts, graphics and follower Q&As centered on the weekly themes.

Grinnell College
Grinnell College is a private liberal arts college known for its rigorous academics and tradition of social responsibility; the college participated in NCSAM in the following ways:

- Individuals and teams signed up for its escape room – “So You Want to Be a Spy?” – and the opportunity to crack codes, discover clues and solve puzzles while learning cybersecurity principles. Sixty people participated in the multiple escape room sessions throughout the month.
- The college handed out Federal Trade Commission brochures and flyers on staying safe online, avoiding scams and dealing with identity theft.
- Grinnell hosted guest speakers from the Office of the Attorney General of Iowa, who gave a talk called “Scam Slam, Detecting and Preventing Fraud.”
- The college held a workshop called “Phishing – Don’t Take the Bait” to help the campus recognize phishing attempts via email and phone. Real campus examples were used.
National Association of State Chief Information Officers (NASCIO)
NASCIO provides state chief information officers (CIOs) and state members with products and services designed to support the challenging role of the state CIO, stimulate the exchange of information and promote the adoption of IT best practices and innovations. NASCIO participated in NCSAM in the following ways:

• Issued a press release for NCSAM announcing its Champion status.
• Had a cybersecurity day at the 2017 NASCIO Annual Conference in Austin, TX. The day consisted of sessions on the human factor and how cybersecurity depends on people and real-world scenarios during which members participated in a debate on real-life simulation.

Princeton University
The information security office at Princeton was active throughout NCSAM, hosting multiple training sessions and opportunities to learn and collect resources about staying safe online. The office’s sessions included topics such as identity theft, securing personal devices and the Internet of Things; the team also created a page dedicated to the month that promoted its activities and 2017 Champion status and links to StaySafeOnline.org resources.

San Diego Cyber Center of Excellence (CCOE) and the City of San Diego
The Cyber Center of Excellence (CCOE) is a nonprofit organization that supplies the leadership and fosters collaboration to establish San Diego as a worldwide center for cybersecurity products and services. The CCOE’s NCSAM activities included:

• Securing San Diego stakeholder forums to facilitate collaboration between the cyber industry, academia and the region’s government, municipalities, utilities and transportation agencies with the mission of fostering a secure cyber environment. The collaborations culminated in the Secure San Diego event for over 200 in-person and 150 online attendees representing industry, academic, government and media stakeholders on Oct. 19, 2017, including:
  o A keynote by William R. Forstchen, the New York Times bestselling author of One Second After.
  o Anatomy of a City Hack – an interactive demonstration of how attackers target regional infrastructure.
  o Hack SD – a panel of San Diego’s critical infrastructure leaders discussing cyber scenarios in comparison to recent global events.
  o SD Acts – a presentation by the region’s emergency response team showing how San Diego government, utilities, companies and academia are working together to mitigate risks.

State of Delaware
The Delaware Department of Technology and Information (DTI) is Delaware’s central IT organization, chartered to deliver core services to other state organizations and exercise governance over the technology direction and investments of the state. DTI participated in the following ways:

• Delaware Gov. John Carney proclaimed October as NCSAM, calling out both DHS and NCSA’s STOP. THINK. CONNECT.™ websites and more.
• DTI conducted its second Food For Thought food truck rally. Patrons of the trucks were quizzed on cybersecurity information while waiting in line to place their food orders.
• The department hosted “Secure Delaware,” a cybersecurity conference for 400 citizens that was held all day and featured three different learning tracks: beginner, advanced and small business.
• TI wrapped a DelDOT coach bus that provides statewide services daily; the theme for the traveling billboard was “Cyber Heroes,” and the billboard was unveiled by Gov. Carney at the cybersecurity conference.
• The department kicked off the “NSA Day of Cyber” challenge in conjunction with former Gov. Markell and Secretary of Education Dr. Bunting.
• DTI provided cyber safety presentations to 4,100 fourth grade students in public, private and parochial schools across the state.
• The department conducted a MS-ISAC poster contest for fourth- and fifth-grade students.
• DTI ran lunch and learn sessions for its employees, statewide information security officers and Information Resource Management Council members.

Texas A&M University
Each October, the Texas A&M Division of Information Technology plans and releases a game for students, faculty and staff in recognition of NCSAM. This year, players were invited to [track a hacker across campus](#) and, with the help of some riddles, try to stop his nefarious actions. More than 9,000 players participated, and more than 7,000 completed the game by answering eight cybersecurity questions and riddles. The division promoted the game across campus using posters, email and social media and even made a [promotional video](#).

University of California, Los Angeles (UCLA)
The UCLA Information Security Office, under the leadership of CISO Michael Story, marked its second NCSAM campaign. During the last two years, UCLA has strived to develop and mature its cybersecurity awareness and education program; its efforts for October 2017 included:

• UCLA issued a campus-wide staff and faculty multi-factor authentication (MFA) mandate. From Oct. 1 to Oct. 31, roughly 30,000 employees enrolled in MFA with help from the IT security team, who led the effort by providing signup assistance during daily “office hours” at multiple locations.

An In-N-Out Burger food truck was on campus on two separate days to help promote and incentivize MFA signups. The 800 students who enrolled received free burgers, chips and beverages. To date more than 6,000 students