Breaking! A Typology of Security and Privacy News and How It's Shared

Sauvik Das
School of Interactive Computing
Georgia Institute of Technology
Atlanta, Georgia, USA
sauvik@gatech.edu

Joanne Lo, Laura Dabbish and Jason I. Hong
Human-Computer Interaction Institute
Carnegie Mellon University
Pittsburgh, PA, USA
jylo@alumni.cmu.edu, {dabbish, jasonh}@cs.cmu.edu

ABSTRACT
News coverage of security and privacy (S&P) events is pervasive and may affect the salience of S&P threats to the public. To better understand this coverage and its effects, we asked: What types of S&P news come into people's awareness? How do people hear about and share this news? Over two years, we recruited 1999 participants to fill out a survey on emergent S&P news events. We identified four types of S&P news: financial data breaches, corporate personal data breaches, high sensitivity systems breaches, and politicized / activist cybersecurity. These event types strongly correlated with how people shared S&P news—e.g., financial data breaches were shared most (42%), while politicized / activist cybersecurity events were shared least (21%). Furthermore, participants' age, gender and security behavioral intention strongly correlated with how they heard about and shared S&P news—e.g., males more often felt a personal responsibility to share, and older people were less likely to hear about S&P news through conversation.

Author Keywords
Quantitative methods; usable privacy and security; news media; cybersecurity; social cybersecurity; privacy

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous;

INTRODUCTION
As cybercrime continues to grow, cybersecurity and privacy (S&P) are becoming increasingly common topics in today's news. One media analytics firm estimates the value of the topics of "online security" and "online privacy" to the global news media to be U.S.D. $617 million and $291 million, respectively [24]. Google Trends estimates the exposure of the "computer security" and "privacy" topics in the worldwide news to be sizable and growing [13], as shown in Figure 1. Indeed, every day we see reports on a cyber-attack that compromises the private information of millions [36], or on national security secrets leaked by whistleblowers [2], or on acts of cyberterrorism [29].

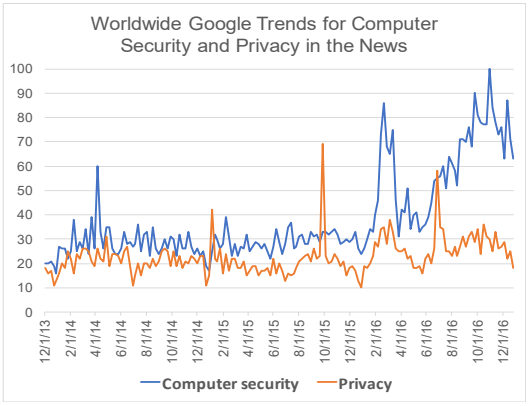

Figure 1. Worldwide Google Trends for the "computer security" and "privacy" topics from December 1st, 2013 to December 31st, 2016. The two topics have steadily been gaining increasing media exposure.

This constant and growing media coverage likely shapes the public's understanding of security and privacy as well as their behavior. Indeed, we know from the well-established theory of agenda-setting [23] that there is a strong connection between media coverage and the societal issues the public finds most salient. Furthermore, we have seen from prior work in usable security [6] that news coverage can often incite S&P behavior change. It is important, therefore, to have a better understanding of *what types of S&P news capture people's attention*, as these news event types likely represent the issues people find most salient.

Additionally, a Pew survey suggests that *how* one hears about news is related to how trustworthy and relevant one finds that news [26]. For example, news sourced from contacts was more often relevant but less often considered trustworthy than news sourced from media companies. Furthermore, prior work suggests that how people *share* S&P news can predict behavior change, as people often share and discuss emerging S&P news before committing to a behavioral response [6]. Thus, it is also important to understand *how people hear about and share S&P news*. So, in this paper, we ask the following research questions:

CHI 2018, April 21–26, 2018, Montréal, QC, Canada

ACM 978-1-4503-5620-6/18/04…$15.00
https://doi.org/10.1145/3173574.3173575

- **RQ1:** What types of security and privacy news do people find salient?
- **RQ2:** How do people generally hear about S&P news? What factors (e.g., age, gender, news event type) correlate with how people hear about this news?
- **RQ3:** In general, when, why and with whom do people share S&P news? What factors correlate with this sharing behavior?

Answering these questions can afford us insights into designing systems that, for example, address the S&P problems people find most salient.

We addressed these questions through a survey study on emerging S&P news events. Over the course of two years, we surveyed participants on Amazon's Mechanical Turk about if they heard about and/or shared emerging S&P news events (e.g., the Panama Papers leak [12], or the Yahoo! email hack [36]). We collected 1999 survey responses for 104 distinct S&P news events through 20 different surveys. To answer RQ1, we employed a mixed-methods clustering analysis on the 104 events in our dataset to create a typology of S&P news. To answer RQ2 and RQ3, we ran a series of quantitative analyses correlating our dependent variables of interest (e.g., how a participant heard about an event and if they shared the event) with four independent variables of interest—demographics (age, gender), security behavioral intention (SBI), and the news event type per our typology.

Our findings suggest that that there are four types of S&P news events that come into people's awareness: financial data breaches, corporate personal data breaches, high sensitivity systems breaches and politicized / activist cybersecurity. Event types strongly correlated with how people heard about and shared news—financial data breaches were shared 42% of the time, while politicized / activist cybersecurity events were shared only 21% of the time. Personal demographics and behavioral factors also strongly correlated with how people heard about security and privacy news (e.g., males were more likely to hear directly from online news sources than females) and people's sharing behaviors (e.g., people with higher SBI were more likely to share S&P news).

Broadly, our work makes two key contributions. First, we introduce a typology of security and privacy news that is salient to the general public. Second, we present a model of how such news events reach people, are shared by people, and how those factors correlate with people's age, gender, SBI and the type of news event. These contributions bridge important insights from the communications and journalism literature to the usable privacy and security literature, and should help both researchers and practitioners design solutions to problems that end-users find important.

BACKGROUND AND RELATED WORK

We drew from literature in journalism, communications and usable privacy and security to construct our research questions. Below, we highlight how our work draws from and builds upon the most pertinent related work.

Communications & Journalism

Dating back to the early 20th century, the communications and journalism literature has emphasized the central role of the media in shaping public opinion [21] and "fostering consensus in society" [20] for many issues of societal importance. Of particular interest to our work is agenda-setting theory, which argues that the news media influences the salience of topics in the public agenda [22]. The seminal paper on the topic, for example, found a 0.9 correlation between the topics discussed by the local press and the topics voters found important in the 1968 U.S. Presidential election [23]. Since then, agenda-setting theory has been found applicable to a variety of non-political domains as well, including: advertising, business news and health communication [22]. There is no reason to believe that news coverage of security and privacy is exempt from these effects. Accordingly, we believe that it is important for HCI researchers to understand the types of security and privacy news coverage that reaches and sticks with the public.

Follow-up studies on agenda-setting argue that there are at least two contingency factors that mediate the effect of press exposure on issue salience: an individual's "need for orientation" and the "obtrusiveness" of an issue. An individual's need for orientation is generally influenced by two factors: *interest* in the topic and *uncertainty* about the message [22,40]. Obtrusiveness captures how much an issue is likely to affect people—highly obtrusive issues are those with which people are likely to have a personal experience (e.g., gas prices) [32]. Accordingly, in our work, we factor in an event's "obtrusiveness" and an individual's "need for orientation" through our typology of security and privacy news events and our measurement of individuals security-related behavior and knowledge.

Usable Privacy and Security Work on Media Influence

Prior work in usable privacy and security alludes to at least three factors that inform people's S&P behaviors: awareness, motivation, and knowledge. Das et al. refer to these factors as an individual's "security sensitivity." [6]

First, many people are *unaware* of security threats and the tools available to protect themselves against those threats [1,35]. News coverage of security and privacy, of course, directly impact the awareness of security threats and tools.

Second, people often have low *motivation* to utilize S&P tools to protect themselves [1,9]. Indeed, prior work suggests that people can have a defeatist attitude towards security, believing that if an attacker wanted to access their data, they could do so irrespective of any counter-measures taken [30,31,39]. Part of this defeatist attitude may be a function of how news coverage presents S&P attacks.

Third, people may not *know* when, why and how to properly practice good security and privacy behaviors. S&P tools are often too complex to operate for those with

Financial Data Breaches	High Sensitivity Systems Breaches	Corporate Personal Data Breaches	Politicized/Activist Cybersecurity
Target Hack (100) Home Depot Hack (21) Wendy's Credit Card Hack (6) Eddie Bauer Credit Card Hack (2) Kmart Credit Card Hack (2) PSN Personal Data Hack (2) Steam Credit Card Hack (2) ADP W-2 Hack (1) Central Hudson G&E Breach (1) Chik-Fil-A Debit Card Breach (1) Citi Customer Account Hack (1) Hyatt Hotels Data Breach (1) Indiana Credit Card Skimmer (1) JC Penney Data Breach (1) Neiman Marcus Card Breach (1) Russian FSB Hack (1) Staples Credit Card Hack (1) SWIFT Bank Malware (1) Trump Hotel Breach (1) UAE Bank Customer Transaction Leak (1) Walmart Credit Card Fraud (1)	Ashley Madison Hack (56) **Adult Friend Finder Hack (4)** **Hollywood Hospital Ransomware (30)** **191 mil Voter Records Exposed (28)** Anthem HealthCare Hack (21) **Brazzer's Hack (16)** **DEA Driver Spying (16)** **93.4 mil Mexican Voter Info Leak (10)** JPMorgan Hack (7) VTech Children's Toy Hack (5) Apple iCloud / Celebrity Photos Hack (4) Medstar Ransomware (4) CareFirst BSBS Personal Data Breach (2) PlayStation / Xbox / Amazon Credit Cards & Passwords Breach (2) Steam DDoS Caching (1) Anonymous KKK Leak (1) Kentucky Hospital Ransomware (1) NCT Credentials Breach (1) NexusMods Customer Data Leak (1) NJ Hospital Ransomware (1) Systema Patient Insurance Breach (1) Three Mobile Customer Fraud (1) Tumblr Hack (1)	**Sony Pictures Entertainment Hack (210)** **500 million Yahoo Accounts (132)** **Dropbox Hack (39)** **Yahoo & Google Email Breach (26)** **GoGo Fake SSL Certs (17)** Generic Corporate Breaches (14) Panama Papers Hack (13) Heartbleed (12) T-Mobile / Experian Breach (6) Verizon Hack (6) Hello Kitty Hack (2) Juniper Networks Backdoor (2) Lastpass Hack (2) Amazon Cloud Key Leak (1) Amazon Kindle Hack (1) Apple Developer Site Hack (1) Facebook Contact Data Leak (1) LinkedIn Credentials Hack (1) Linux Mint WordPress Hack (1) LizardStresser Customer Data Leak (1) MacKeeper Hack (1) Patreon Credentials Hack (1) Snapchat Photos Leak (1) Spotify Hack (1) Time Warner Login Credential Hack (1) Tumblr Email Breach (1)	**Apple's Letter on Encryption (67)** **CENTCOM Social Media Hack (59)** **Anonymous vs ISIS** **Obama Security Announcement (47)** **FBI Employee Hack (35)** **France Blocking Free Wi-Fi (25)** DNC Email Leak (19) **Krebs Mirai IoT DDoS Attack (18)** IRS Identity Theft (17) **John Oliver Encryption Skit (17)** OPM Personal Data Breach (14) Clinton Email Server (11) **55 mil Filipino Voter Info Leak (7)** Snowden (4) China U.S. Security Tensions (3) EA / Blizzard DDoS (3) PSN / Xbox Live outage (3) USPS Data Breach (3) Bowman Avenue Dam Hack (2) FDIC Hack (2) Adele Photos Hack (1) Anonymous Canadian Government Takedown (1) EU Airport Leak (1) FancyBears Athlete Doping Leak (1) German Parliament Hack (1) HSBC DDoS Attack (1) Jester Jihadist Attacker (1) Leaked Police Union Contracts (1) Steam Password Reset Hack (1) Twitter State Sponsored Hackers (1) U.S./U.K Hack Own Bank (1) Uber Driver Leak (1) US Russia Security Meeting (1) Wells Fargo Hack (1)

Table 1. A list of all S&P news events in our sample, organized by the high-level types we propose in our S&P news typology. The typology was constructed through a mixed-methods analysis of all 104 news events. Bolded events are the original 20 events we asked about in our surveys. Events are sorted in descending order of how many participants reported hearing of the event (reported in paraentheses next to the event name).

high security sensitivity [41]. Poorly sourced news can worsen the situation. Wash found that people hold "folk" models of computer security that are often misguided—sometimes because of poorly sourced news—and use these faulty models to justify ignoring security advice [39].

Each of these three factors—awareness, motivation and knowledge—may be affected in some way by S&P news coverage. Indeed, some prior work in usable security has highlighted that security and privacy news events can catalyze both conversations and behavior change [6]. Despite the importance of S&P news coverage in informing end-user perceptions and behavior, however, we could find little work that has been done on understanding cybersecurity and privacy news coverage more broadly, nor how that coverage reaches and spreads among people.

Our work contributes to the literature in usable privacy and security by providing a typology of S&P news along with a model of how that news reaches and spreads among different types of end-users. We expect these models to be useful in informing the design of solutions to the security and privacy problems that people find most salient.

METHODOLOGY

We selected 20 emergent news events about cybersecurity and privacy that gained widespread coverage in between December 2014 and December 2016. For each of these events, we asked 100 participants on Amazon's Mechanical Turk platform to fill out an 8-minute survey. Responses to these 20 surveys constituted our dataset. Below, we describe our event selection procedure and our survey.

Sampling Security and Privacy News Events

Our strategy to select emergent S&P news events was multi-faceted: (i) we set up a Google News alert for the keywords that were part of the "computer security" and "privacy" topics on Google Trends, including "cybersecurity", "information security", "privacy", "information privacy" and "internet security"; (ii) we monitored popular news media websites that often write and/or distribute content about security and privacy (e.g.,

Hacker News, The Atlantic, VICE Motherboard, Ars Technica); (iii) we closely followed security and privacy journalists and/or bloggers on social media; (iv) we joined mailing lists in which news about security and privacy was often distributed; and, (v) we asked survey respondents to recall a recent news event about security and privacy that had come to their attention if they had not heard about the event in response to which we ran the survey.

We selected twenty events that were covered by multiple outlets and were shared at least 1000 times on social media (as calculated by the Facebook and Twitter share button counters on the articles). Ultimately, the events we selected covered a broad spectrum of security and privacy news, including: news of personal data breaches (e.g., the Yahoo! email hack [36]), government surveillance (e.g., Apple's open letter on encryption in response to the San Bernardino shootings [16]) and humor pieces (e.g., John Oliver's skit on encryption [28]). Apart from these events, we collected data on an additional 84 distinct news events contributed by 664 survey respondents who had not heard about the event for which they were taking a survey. Table 1 lists all of these events. Appendix A, in the supplementary documents, provides a short description of each.

Just-in-Time Surveys

To better understand how people come to hear about security and privacy news, as well as if and how people share these events with others, we ran "just-in-time" surveys with 100 respondents after each of the 20 news events we selected. These surveys were "just-in-time" in that they were run about seven days after the selected news event was first publicized in order to balance the "freshness" of an event in participants' minds while still allowing enough time for an event to propagate to a broad audience. The specific questions asked in the survey are provided in Appendix B of the supplementary documentation. Due to space constraints, we provide a high-level overview of the questions asked below.

Event questions: We first asked participants if they had heard about the selected news event. If participants had *not* heard about the event in question, we asked them to provide a link to a different security or privacy news event that had recently come to their attention. If they did so, they would answer the subsequent questions in relation to *that* event. If participants had not heard about the original event and could not recall an alternative, they were forwarded to the final two sections of the survey in which we collected demographic and behavioral information.

Source question: Participants who had a reference event in mind (either the original event we asked about or an alternative event that had come to their mind) were then asked questions about how they heard about the event. Borrowing from Das et al.'s typology of catalysts for security behavior change and conversations [6], respondents could select from the following (paraphrased) options: (i) from an online news article, (ii) directly from someone else, (iii) from a social media post, (iv) from a television broadcast, or (v) from a company / service provider. If none of those options applied, participants could manually specify the source. Participants were allowed to select multiple sources.

Social Source Questions: Options (ii) and (iii) of the aforementioned source question were considered *social* sources. Participants who selected a social source were asked a few additional questions about their source and how their source shared information about the event.

First, participants were asked to specify *who* was that social source: friend, family member, significant other, or colleague. Then, participants were asked to specify *how* the source shared information with them: face to face, SMS/email, phone call or social media. Finally, participants were also asked *what* the source shared: general information about the breach, solutions, advice or best practices to protect oneself against the breach, a story about the breach, or venting about how they were personally affected by the breach. The provided options were, again, motivated by the typology of security conversations introduced by Das et al. [6] Participants could select multiple answers for any of the questions. Participants could also manually write in an answer for any of the questions, if none of the provided options were applicable.

Share question: Participants were then asked if they shared the news event with others. If they did, we asked participants questions about *who* they shared the event with, *how* they shared it, *what* they shared and *why* they shared it. For the *who*, *how* and *what* questions, participants could select from the same set of options as specified in the social source questions above. For the *why* question, participants could select from: I noticed they were behaving insecurely and wanted to warn them; I wanted to provide them with information on how to protect themselves from the breach; I felt a responsibility to protect them; I experienced the breach myself; and, I read an article about the breach. Participants could select multiple options, and, again, could write in an answer if necessary.

Security behavioral intention questions: A goal of ours was to correlate what Das et al. call "security sensitivity" [6] with how people hear about and share security and privacy news. As we briefly mentioned in the related work section, *security sensitivity* broadly encompasses people's awareness of security threats, motivation to act in defense against those threats, and their knowledge of how to act in defense against those threats. Unfortunately, there is, as yet, no scale that specifically measures security sensitivity, so we used scales that measured related concepts instead.

For the first five surveys we ran, we used three scales—measuring security behavior, literacy and knowledge—first introduced and validated by Kang et al. [18] The behavior scale consisted of 11 yes/no questions probing whether or not one engaged in common security and privacy behaviors

(e.g., "I have used a service that would help me browse the internet anonymously, such as a proxy server, Tor, or a VPN"). The literacy scale asked participants how familiar they were with 9 concepts in consumer-facing cybersecurity and online privacy (e.g., onion routing, VPNs, encryption) on a 5-point Likert-scale ranging from "I have never about this" to "I know very well how this works". Finally, the knowledge scale consisted of 8 true/false quiz questions in which we tested knowledge of consumer-facing cybersecurity (e.g., "Private browsing mode in browsers prevent websites from collecting information about you.").

For the latter 15 surveys we used the security behavioral intention scale (SeBIS), a validated and parsimonious scale that measures people attitudes towards enacting good security behaviors. [10]. As security behavioral intention is related to security sensitivity, we considered the SeBIS a good proxy for security sensitivity. Accordingly, we started using the SeBIS after it was publically released in May of 2015. We explain how we account for this change in scale usage in our analysis in the "Computing Security " subsection.

Demographic questions: Finally, participants were asked a number of demographic questions about their *age*, *gender*, whether or not they worked in a *cybersecurity related field*, and whether or not they had *native proficiency* in English. Participants were given the option to not answer these questions if that was their preference.

Recruitment

We recruited a total of 1999 participants from Amazon's Mechanical Turk, or ~100 for each of the twenty surveys we ran. We recruited a unique set of participants for each survey. We also restricted participation to only those within the U.S. as we expected the news sources we monitored to be skewed towards topics of interest to the U.S. public. We titled the HIT for *all* of our surveys "Answer a 10-minute survey about cybersecurity and/or privacy breaches" with a description of "We will ask you a few questions about recently publicized cybersecurity or privacy breaches." We compensated participants $1 for completing the survey, which took about eight minutes on average. Our study protocol was approved by an institutional review board.

We used Mechanical Turk because of its readily available population of Internet savvy users that we expected to persist throughout our data collection. We note, however, that there are some differences between Mturkers and the general U.S. population [17]—the former is more internet savvy and has higher privacy concern than the latter.

DATASET

Descriptive Demographics

Our sample of 1999 participants across the 20 surveys included a fairly wide spread of ages—70% of participants were within 25-45 years old. Our sample consisted of 1145 (57%) males, 847 females and 7 participants who preferred not to answer. It is also notable that 605 participants (34%) in our sample had a computer science, cybersecurity or engineering related occupation, which is an over-representation of tech savvy individuals. We suspect this skew is a result of topical self-selection: our survey titles included the terms cybersecurity and privacy. Finally, 1992 participants reported native level proficiency in English.

Reference events

Out of the 1999 survey responses we collected, 729 (37%) were from participants who *had* heard about an event we selected, 664 (33%) responses were from participants who had *not* heard about the selected event but provided an alternative reference event, and 606 (30%) were from participants who had not heard about the event we selected and also could not recall any other recent incident.

Two researchers independently went through each of the 664 links to alternative reference events and found an additional 84 distinct news events about security and privacy. Thus, in total, our dataset comprised of 104 distinct security and privacy news events.

Computing Security Behavioral Intention

We wanted to understand if people who had more or less security sensitivity differed in how they heard about and shared S&P news. To facilitate this analysis, we computed a single score approximating security sensitivity for each of our survey respondents. Recall, however, that we used two different sets of questions to measure security sensitivity: a combination of the knowledge, behavior and literacy scales proposed by Kang et al. [18] in the first five surveys and the SeBIS [10] for the latter fifteen.

To calculate a single value that represented security sensitivity, we used a structural equation model using R's lavaan package [33]. We modeled each of the questions of the knowledge, familiarity and behavior scales as feeding in to a latent factor measuring knowledge, familiarity and behavior, respectively. Those three sub-factors, in turn, fed into a single, higher-level latent factor. For the SeBIS, we used the model provided by the original paper [10]: the 16 questions in the scale fed into 4 sub-factors which, in turn, fed into one higher-level factor. We used the factor scores for these higher-level factors, in both models, as an estimate for a participant's overall security behavioral intention (SBI) which was our proxy for security sensitivity.

RESULTS

What types of S&P news do people find salient?

To begin creating a typology for security and privacy news events, two researchers collaborated in an open-coding process [25]. First, both researchers coded the initial 20 news events to identify pertinent dimensions of interest. Then, both researchers independently coded 75 news events each, with 50 of the events overlapping, focusing on identifying codes within the mutually selected dimensions of interest. The two researchers then came together and discussed points of disagreement in the codebook until they both agreed upon a final codebook and then applied the final codes to all 104 news events.

Through this process, we identified three key dimensions of S&P news and 29 codes within those dimensions that typified different security and privacy news events. These dimensions are described in more detail below. For brevity, we don't describe each code in detail. Appendix C of the supplementary documents presents each code, a detailed definition and an example event exemplifying the code.

Responsible Parties: Who was responsible for the incident described in the news event? The *six* codes for this dimension were: a corporation; domestic government (from the point of view of the article); foreign government (from the point of view of the article); hacktivists / vigilantes / whistleblowers; journalists; and, personally-motivated attackers / researchers.

Primary Topic: How can the event best be described? The *ten* codes for this dimension were: account credentials leak; celebrity data breach; cyberwarfare; denial of service; financial data / resource breach; government surveillance; legislation; personal account / data breach; ransomware; and, security implementation bug.

Context: What are pertinent contextual factors that might explain or affect the event? The *thirteen* codes for this event were: big-brother government; children; corporate security; election; financial institution; foreign affairs; gaming; government / national security; medical institution; point-of-sale hack; race violence; sexual life; and, terrorism.

Next, to get a better sense of how these different codes interrelated, we formed clusters of related events based on their codes. To do so, we started by constructing a binary feature vector for each news event. For each of the aforementioned qualitative codes, a news event would receive a *1* if the code was present and a *0* otherwise, resulting in a 104x29 binary matrix. We next constructed a graph of the news events and their codes. Each vertex was one of the 104 news events. Edges between vertices were weighted, where the weight was calculated based on the Pearson correlation of the code vectors for the two news events. Accordingly, news events that were assigned similar codes would have an edge with strong weights and vice versa. To ensure positive weights, we scaled the Pearson correlation between the values of 0 and 1.

This process constructed an undirected, weighted network on which we ran a Louvain modularity community detection algorithm [4] to find "communities" of news events that are broadly similar in terms of the codes we refined. The Louvain method is advantageous over methods such as k-means clustering in that it is deterministic and the number of clusters need not be known ahead of time.

This analysis yielded four categories of news events, which we describe below. The names of these categories represent our best attempt to represent the **shared qualitative codes** among the events in a category. Note that all of the events that fell into each of the types are listed in Table 1.

Politicized / activist cybersecurity (34 / 104) news encompassed a broad range of incidents that were generally politicized or activism-inspired. These news events were an eclectic mix, with each of the dominant codes generally applying to a small subset. Specifically, the dominant codes for these events were hacktivists / whistleblowers / vigilantes (9/34), national security (7/34), cyberwarfare (8/34) and denial-of-service (6/34). Events that fell into this category include: the U.S. CENTCOM (U.S. Central Command) Social Media Hack [34], in which foreign nationalists compromised CENTCOM's Twitter account; and, the hacking collective Anonymous' declaration of war against ISIS following terror attacks in Paris [7].

Corporate personal data breaches (26 / 104) were characterized by three dominant codes: personal account / data breaches (20/26), corporate security (26/26), and account credential leaks (4/26). As the name of the cluster and its dominant codes suggest, these events broadly entailed the stealing of personally identifiable information, account information and other personal data held by end-user facing companies. Examples of these breaches include the Panama Papers Leak [12], in which a Panamanian law firm was attacked and had their customers' confidential documents leaked; and, the Yahoo! Hack [36] in which over a billion Yahoo! email accounts were compromised.

High sensitivity systems breaches (23 / 104) included news coverage on attacks that compromised the personal information of vulnerable populations (e.g., the VTech Children's Toy hack that leaked children's personal data [37]), leaks of highly private personal information (e.g., the Ashley Madison hack that exposed members of the extramarital dating website [42]), or attacks targeted against medical institutions (e.g., the Hollywood Presbyterian Medical Center ransomware attack [38]). The dominant codes for these events were medical institutions (8/23), ransomware (4/23), personal account / data breaches (18/23) and sexual life (4/23).

Financial data breaches (21 / 104) involved the leaking of sensitive financial data, such as credit cards or tax returns. Examples of financial data leaks include the Target [27] and Home Depot [3] credit card hacks, in which millions of customers' credit card details were compromised. Financial data breaches were characterized by the following dominant codes: financial data / resource breach (21/21), corporate security (7/21) and point-of-sale hacks (8/21).

In summary, through a mixed-methods coding and clustering of the 104 news events in our dataset, we uncovered four broad types of security and privacy related news events that seem to be salient to the public: (i) politicized / activist cybersecurity, (ii) corporate personal data breaches, (iii) high sensitivity systems breaches, and (iv) financial data breaches. Again, Table 1 lists each of these categories and all their member events.

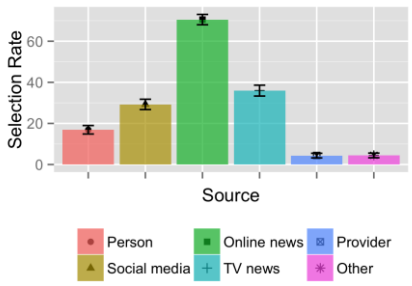

Figure 2. Distribution of how participants reported hearing about security and privacy news events. Most people heard about news events through online news sources.

How do people hear about S&P news events?

To answer the question of how people generally tend to hear about security and privacy news events, we analyzed the responses from the 729 participants who had heard of one of the news events we selected as well as the 664 who wrote in an alternative event. Unfortunately, due to technical difficulties that prevented us from storing some responses to one of the surveys—the survey in response to Anonymous' declaration of war against ISIS—we excluded data from that survey in our analyses where those responses were required. Furthermore, 47 of the responses among the 664 who wrote in alternative news events did not provide enough information for us to find the alternative event in question. Ultimately, our dataset consisted of 1265 responses to known security and privacy news events.

Figure 2 shows how participants heard about security and privacy news events. In general, people reported primarily hearing about the news event directly from reading an online news article (70%), followed by television news (36%), social media (29%), directly from another person (17%) and, lastly, from a service provider (e.g., ISP or corporation) (4%). An additional 4% wrote in an alternative source. These participants primarily reported hearing about news events from radio broadcasts or print media. Note that participants could select more than one option, resulting in the percentages adding up to more than 100%.

Next, to evaluate if and how people with different demographics and security behavioral intention (SBI) differed in how they heard about S&P news events, as well as to uncover any pairwise differences between news event types, we ran a multivariate logistic regression (i.e., with multiple related dependent variables, or DVs) [14] with a random intercept for news event. The regression had five binary DVs corresponding to the sources participants selected (i.e., another person, TV news, social media, a service provider, an online news source).

Our model had four independent variables (IVs): age, gender, event type, and SBI. We calculated six pairwise comparisons between the different four event types using a contrast matrix with R's multcomp package [15].

	Online News	Another Person	Social Media	TV / Video	Service Provider
Intercept	**0.93˚**	**-0.97˚**	-0.29	**-1.28˚**	**-3.01˚**
Individual-level variables					
Age	**-0.10***	**-0.20˚**	**-0.24˚**	**0.21˚**	0.13
Male (vs. Female)	**0.35†**	-0.21	-0.04	-0.13	**-0.89†**
Security Behavioral Intention	**0.38˚**	-0.11	-0.11	-0.12	0.04
Event-type comparisons					
F vs. C	0.42	0.29	0.36	0.17	0.61
P vs. C	0.02	0.04	0.20	-0.22	**-0.79***
S vs. C	-0.12	0.27	-0.40	0.01	-0.08
P vs. F	-0.41	-0.25	-0.16	-0.39	**-1.40†**
S vs. F	-0.54	-0.02	**-0.76***	-0.16	-0.69
S vs. P	-0.14	0.23	**-0.60***	0.23	0.70

Table 2. Logistic regression coefficients of information source modeled against individual-level factors and event-type comparisons. Rows represent IVs, columns DVs. Both individual-level factors (age, gender, security behavioral intention) and event-types significantly correlated with how people heard about news events.

*˚p<0.001 † p <0.01 * p<0.05*

F=financial data breaches, C=corporate data breaches, S=high sensitivity systems breaches, P=politicized / activist cybersecurity

Significance levels were calculated using Bonferroni correction to account for multiple testing. Results from this regression are shown in Table 2.

Coefficients for the numeric IVs (i.e., age, SBI) indicate a change in log odds, or $\ln(\frac{P}{1-P})$, where P represents the probability that a participant heard about a news event from a particular source. A positive coefficient implies that the log odds that a participant heard about a news event from one source increases as the predictor variable increases by one standard deviation (i.e., P increases), while a negative coefficient implies the opposite (i.e., 1-P increases). For example, for the online news source, the age variable ($b_{news}^{age} = -0.10$) has a negative coefficient. Thus, for every one-standard deviation increase in age, a participant's log odds to have heard about a news event through an online news source decreases by -0.10.

For categorical IVs (i.e., event-type comparisons, gender), coefficients represent the difference in log-odds that a participant heard from a particular source between participants at two different levels of the IV (e.g., male vs female). For example, the log odds for participants to hear about a high sensitivity systems breach versus a financial data breach on social media is lowered by $b_{social}^{SvsF} = -0.76$.

As we suspected, our analysis revealed that both individual-level factors and event type were significant correlated with how people came to hear about security and privacy news events. Indeed, younger people were more likely to hear directly from online news ($b_{news}^{age} = -0.10$), through

	Coefficient	*p value*
Intercept	**-0.76**	**0.002**
Individual-level variables		
Age	-0.02	0.73
Male (vs. Female)	-0.15	0.27
Security Behavioral Intention	**0.26**	**<0.001**
Event-type comparisons		
F vs. C	0.35	0.26
P vs. C	-0.40	0.10
S vs. C	-0.41	0.09
P vs. F	**-0.75**	**0.02**
S vs. F	**-0.76**	**0.02**
S vs. P	0.01	0.96

Table 3. Logistic regression of decision to share modeled against individual-level factors and event type comparisons. Rows represent IVs. People with higher SBI were more likely to share news events, and some event types had significantly different sharing rates.

F=financial data breaches, C=corporate data breaches, S=high sensitivity systems breaches, P=politicized / activist cybersecurity

another person ($b_{person}^{age} = -0.20$), and through social media ($b_{social}^{age} = -0.20$), while older people are more likely to hear through television news sources ($b_{tv}^{age} = 0.21$). Males were more likely to hear about security news events directly from online news source ($b_{news}^{male} = 0.35$), but less likely to hear from service providers ($b_{sp}^{male} = -0.89$). And, people with higher SBI were much more likely to hear about security news events through online news sources ($b_{news}^{sbi} = 0.38$). As online news sources and social media are often the first to pick up and spread news, these findings suggest that younger people, males, and those with high SBI are the early audience for S&P news.

Different event types were also more or less likely to spread through different sources. Most notably, both financial data leaks and politicized / activist cybersecurity were more likely to spread through social media than high sensitivity systems breaches ($b_{social}^{SvsF} = -0.76, b_{social}^{SvsP} = -0.60$), suggesting these two event types are more likely to spread virally online. Furthermore, both financial data breaches and corporate personal data breaches were more likely to spread through service provider correspondences than politicized / activist cybersecurity ($b_{sp}^{PvsC} = -0.79, b_{sp}^{PvsF} = -1.40$), suggesting that these two event types are more likely require direct action.

From who and how do people hear about news events?

As mentioned above, about 29% of our participants selected social media as a source, and 17% selected hearing directly from someone else. Analyzing these participants' answers to the social source questions, we found that people primarily heard from friends (64%). Fewer heard from family (16%), significant others (12%) and colleagues (13%). The second most populous selection was the "other" category (18%). Unpacking this category, participants described strangers and/or third-party organizations whose post came to their attention on social media.

In addition, participants reported primarily hearing from their social sources through face-to-face communication (72%) or social media (35%).

In sum, when participants hear about security and privacy events from others, they hear primarily from friends and, surprisingly, in a face-to-face conversation. Interestingly, people rarely hear about security and privacy from family members or significant others, suggesting that security and privacy are not topics often discussed with loved ones.

How, why and with whom do people share S&P news?

Out of the 1265 respondents who had heard about a recent security news event, 303 (29%) also reported sharing that news event with others. To evaluate if people with different demographics and security behavioral intention differed in if and how they shared security and privacy news events, as well as to statistically test pairwise differences between news event types, we ran another logistic regression with random intercepts for each event.

The DV was a binary value indicating if a participant shared a news event, and the IVs were age, gender, security sensitivity and event type. We again calculated the six pairwise comparisons between the four different event type's using a contrast matrix with R's multcomp package [15]. Significance levels were calculated using Bonferroni correction to account for multiple testing. Results from this regression are shown in Table 3. Coefficients can be interpreted as explained in the previous analysis.

From Table 3, we can see that while age and gender were not significantly correlated with sharing a news events, security behavioral intention did significantly correlate with sharing. Specifically, people with higher SBI were significantly more likely to share security and privacy news events ($b_{share}^{sbi} = 0.26$)—an unsurprising finding, and one that reaffirms the notion that experts do try to share their knowledge with an interested audience, despite feeling a need to censor themselves as suggested in prior work [6].

The type of event in question was also significantly correlated with the likelihood of sharing news. To ease interpretation of the coefficients for event-type comparisons in Table 3, we also calculated overall sharing rates by event type. Financial data braches were the most shared events (42%), followed by corporate personal data breaches (33%), high sensitivity systems breaches (24%) and finally politicized / activist cybersecurity (21%). From the regression analysis in Table 3, the differences in sharing rate between financial data breaches and the latter two event types were found to be significant. These sharing frequencies appear to relate to the immediate relevance of an event to the average individual—i.e., "obtrusiveness". More obtrusive issues that could potentially warrant action from an average person (e.g., credit card hacks or email account credential leaks) are shared more frequently than

	Intercept	Age	Male (vs. female)	SBI
Friend	0.21	-0.04	**0.47***	-0.16
Family	0.21	-0.02	-0.12	0.16
Sig. Other	-0.44	0.03	**-0.66†**	**0.30***
Colleague	**-1.97˚**	0.01	**0.60***	**0.33***

Table 4. Multivariate logistic regression coefficients of selected audience modeled against individual-level factors. Rows represent DVs, columns IVs. Males were more likely to share with colleagues, and females with significant others. People with high security behavioral intention were more likely to share with colleagues *and* significant others.

*˚p<0.001 † p <0.01 * p<0.05*

less obtrusive issues that are not actionable (e.g., compromised hospital systems).

With whom do people share S&P news events?

People who shared news events primarily shared with friends (59%) and family (53%), followed by significant others (34%) and colleagues (19%).

We next analyzed if there was a significant correlation between a participant's intended audience and the participant herself. Table 4 shows the regression coefficients for a multivariate logistic regression with random intercepts for each event. These regressions modeled the audience with which participants shared information about security events against their age, gender and security behavioral intention. Coefficients can be interpreted in the same way as in previous analyses.

We can see that gender and SBI were correlated with audience selection. Specifically, males were more likely to share security and privacy news events with colleagues and friends ($b^{male}_{colleague} = 0.60, b^{male}_{friend} = 0.47$), while females were more likely to share events with significant others ($b^{male}_{sigother} = -0.66$). People with higher SBI were more likely to share news events with both significant others and colleagues ($b^{sbi}_{sigother} = 0.30$, $b^{sbi}_{colleague} = 0.33$).

Recall, however, that participants rarely reported hearing about S&P news from family and significant others. This asymmetry in our participants' sharing of S&P news with friends, family and significant others but only hearing of S&P news from friends may be an artifact of our sample, which over-represents people who work in technology-related fields. If so, this finding adds to the evidence that more technically savvy people want to share information about security and privacy with loved ones, but usually have to initiate those conversations.

Why do people share S&P news events?

Among participants who reported sharing a news event, most mentioned that they did so because they just wanted others to read an article about the event (67%). The second most common reason was to provide specific advice (23%), followed by a feeling of responsibility to share the information (15%), simply sharing a personal experience with others (10%) and noticing that other people were behavior in a manner that was insecure (3%).

	Intercept	Age	Male (vs. female)	SBI
Noticed Insecure Behavior	**-5.16˚**	0.10	0.93	**-1.03†**
Share info to protect	**-1.30˚**	0.05	-0.19	0.27
Felt personal responsibility	**-2.49˚**	0.10	**0.72***	-0.21
Share personal experience	**-1.72˚**	-0.05	-0.68	-0.18
Share article on event	**0.92†**	-0.13	0.37	0.25

Table 5. Multivariate logistic regression coefficients of reason for sharing modeled against individual-level factors. Rows represent DVs, columns IVs. Males were more likely to feel a personal responsibility to share news. Curiously, people with lower security behavioral intention were more likely to share when they noticed others' insecure behavior.

*˚p<0.001 † p <0.01 * p<0.05*

We ran a final multivariate logistic regression analysis with random intercepts for each event to correlate rationales for sharing with individual-level factors. Table 5 shows the results, and coefficients can once again be interpreted as in previous analyses. Again, age was not correlated with rationale for sharing but gender and SBI did correlate. Specifically, we found that males were significantly more likely to share news events because they felt a personal responsibility to do so (b=0.72, p=0.03) and that, surprisingly, people with *lower* SBI were more likely to share a security news event because they noticed others behaving insecurely (*b*=-1.03, p=0.01).

DISCUSSION

What type of security and privacy news do people find salient? How do people hear about this news? Why, how and with who do people share this news? We attempted to answer these questions in order to better understand the S&P issues that people find important; how they come to know about these issues; and, with who, how and why people communicate about security and privacy. Below, we list our key findings and some potential implications.

1. **There are four broad types of security and privacy news events that comprise the S&P "agenda" the media pushes to the public.** *Financial data breaches* encompass news events about compromised financial information or resources: for example, leaked credit card numbers, tax returns, or bank account information. *Corporate personal data breaches* encompass news events about corporations that were compromised and had customer data stolen: for example, leaked account credentials or personal information. *High sensitivity systems breaches* cover attacks on vulnerable populations (children), hospitals or on activities that are considered highly sensitive (sexual activities). Finally, *politicized / activist cybersecurity*

encompasses topics on cyberwarfare, whistleblowing or hacker groups that act on political motivations.

Prior work has highlighted that S&P is often promoted through fear, uncertainty and doubt (FUD) [11] and our typology of S&P news provides some supporting evidence for that claim. Indeed, these four distinct categories share a commonality: they are reactions to S&P breaches that are often beyond the *agency* of any individual. In other words, the media agenda for S&P may be one that calls into question the efficacy of individual S&P behaviors. What good is a stronger password if a large company or government agency is compromised and leaks one's personal information anyway? Proactive security behaviors are important to limit the damage these breaches can cause, but this simple message may be lost amidst never-ending reports on the latest big security breach.

A possible design implication, then, is the need to promote greater agency in S&P — i.e., there should be a clear connection between an individual's S&P behaviors and the (lack of) consequences for relevant news events. Indeed, prior work suggests that individual agency improves the acceptance and efficacy of security tools [8]. One way this could be accomplished, for example, is through tools that promote useful S&P behaviors that counteract relevant S&P breaches: for example, in the wake of the Yahoo! email breach, a password manager might notify a user that she should change her Yahoo! account password to reduce the damage the breach can cause.

2. **Individual differences correlate with how people hear about security and privacy news as well as how, why and with who people share this news**. Older people, for example, were more likely to hear about S&P news through television, while younger people were more likely to hear about these events through online news sources. Males were more likely to hear directly from online news sources and to share events with friends and colleagues, while females were more likely to share with significant others. People with higher security behavioral intention were more likely to learn about news events directly from online news sources and more likely to share S&P news, in general.

These findings suggest that different people can have different information diets for S&P, and prior work suggests that these information diets may affect their security sensitivity [6]. A possible direction, then, is to design security tools that utilize these differences in information diets to personalize S&P recommendations in a way that is balanced against end-users' expectations of privacy [19]. One example would be a tool that recognizes that a user is less likely to hear about a relevant breach based on her personal information diet and informs her of the event and ways to protect herself through other means.

3. **People sometimes share news events to provide advice or because they feel a personal responsibility.** The most commonly reported reason to share S&P news was to get others to read an interesting article. However, the second most prevalent reason was to provide advice, and the third was that people felt a personal responsibility.

This finding provides supporting evidence to the growing body of literature highlighting the need for tools that facilitate *stewardship* in cybersecurity—or, the ability to act in benefit of another's S&P. Prior work [5,6] has noted that some people feel a sense of accountability for the security and privacy of their loved ones, but few solutions exist. One possibility would be a tool that would allow experts to make changes or suggestions on behalf of consenting friends in the wake of a relevant S&P breach—for example, strongly urging a password reset on affected accounts.

LIMITATIONS

As with any study, ours has its limitations. The first is sampling bias: our respondents were all Mturkers who self-selected into doing a HIT to answer questions about recent S&P related news events. Prior work suggests that Mturkers have higher levels of security and privacy concern and internet usage than the general U.S. population [17].

Another limitation is our consolidation of multiple different scale items to measure security sensitivity. We did so primarily because the SeBIS [10] was released after we had begun our data collection.

Our analysis of how event-level factors correlate with how people hear about and share S&P news did not take into account many variables that warrant further investigation: e.g., the severity of an event. We also did not capture how these news events actually affected people's S&P behavior outside of sharing the news event with others.

CONCLUSION

News media coverage of cybersecurity and privacy is significant and growing, and this coverage likely affects end-users' perceptions and behaviors. To better understand what types of security and privacy news events are salient to people, we collected and analyzed 1999 survey responses for 104 distinct S&P news events over the course of two years. Through this work, we made two key contributions. First, we proposed a typology of security and privacy news events. Second, we presented a model of how such news events reach people, are shared by people, and how those factors correlate with people's age, gender, security behavioral intention, and the type of news event. These contributions should help HCI researchers and practitioners design solutions that address problems that everyday people find especially salient and important. For example, in the creation of systems that allow for stewardship, systems that personalize S&P recommendations to each individual based on their unique information diets, and systems that promote individual agency.

ACKNOWLEDGMENTS

This work was generously funded by NSF Grant #1347186. Special thanks to Tiffany Kim and Erik Harpstead for participating in helpful discussions throughout the project.

REFERENCES

1. Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Communications of the ACM (CACM)* 42, 12: 40–46. http://doi.org/10.1145/322796.322806
2. James Ball, Julian Borger, and Glenn Greenwald. 2013. Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
3. Shelly Banjo. 2014. Home Depot Hackers Exposed 53 Million Email Addresses. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/home-depot-hackers-used-password-stolen-from-vendor-1415309282
4. Vincent D Blondel, Jean-Loup Guillaume, Renaud Lambiotte, and Etienne Lefebvre. 2008. Fast unfolding of communities in large networks. *Journal of Statistical Mechanics: Theory and Experiment* 2008, 10. http://doi.org/10.1088/1742-5468/2008/10/P10008
5. Sauvik Das. 2016. Social cybersecurity: Understanding and leveraging social influence to increase security sensitivity. *it - Information Technology* 58, 5: 237–245. http://doi.org/10.1515/itit-2016-0008
6. Sauvik Das, Hyun Jin Kim, Laura A. Dabbish, and Jason I. Hong. 2014. The Effect of Social Influence on Security Sensitivity. *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS'14)*.
7. Anna Dubuis. 2015. Anonymous declares war on Islamic State after Paris attacks in chilling video: "We will hunt you down." *The Mirror*. Retrieved from http://www.mirror.co.uk/news/world-news/anonymous-declares-war-islamic-state-6839030
8. W. Keith Edwards, Erika Shehan Poole, and Jennifer Stoll. 2008. Security automation considered harmful? *Proceedings of the 2007 Workshop on New Security Paradigms - NSPW '07*, ACM Press, 33. http://doi.org/10.1145/1600176.1600182
9. Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. *Proc. CHI '08*, ACM Press, 1065. http://doi.org/10.1145/1357054.1357219
10. Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proc. CHI'15*, ACM Press, 2873–2882. http://doi.org/10.1145/2702123.2702249
11. Dinei Florêncio, Cormac Herley, and Adam Shostack. 2014. FUD: A plea for intolerance. *Communications of the ACM* 57, 6: 31–33. http://doi.org/10.1145/2602323
12. Juliett Garside, Holly Watt, and David Pegg. 2016. The Panama Papers: how the world's rich and famous hide their money offshore. *The Guardian*. Retrieved from https://www.theguardian.com/news/2016/apr/03/the-panama-papers-how-the-worlds-rich-and-famous-hide-their-money-offshore
13. Google. 2017. Worldwide Trends for Computer Security and Privacy in the News. Retrieved from https://trends.google.com/trends/explore?date=2013-12-01 2016-12-31&gprop=news&q=%2Fm%2F06804,%2Fm%2F022x_
14. Joseph Hair, Rolph Anderson, and William C. Black. 2006. *Multivariate Data Analysis*. Prentice Hall.
15. Torsten Hothorn, Frank Bretz, Peter Westfall, Richard M. Heiberger, Andre Schuetzenmeister, and Susan Scheibe. 2017. Simultaneous Inference in General Parametric Models. Retrieved from http://multcomp.r-forge.r-project.org
16. Kevin Johnson. 2016. Privacy debate overshadows what's on San Bernardino killer's phone. *USA Today*.
17. Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy Attitudes of Mechanical Turk Workers and the U.S. Public. *Proc. SOUPS'14*, 37–49.
18. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My data just goes everywhere": User mental models of the internet and implications for privacy and security. *Symposium on Usable Privacy and Security (SOUPS) 2015*, 39–52.
19. Alfred Kobsa. 2007. Privacy-Enhanced Personalization. *Communications of the ACM (CACM)* 50, 8: 24–33. http://doi.org/10.1145/1278201.1278202
20. Harold D Lasswell. 1948. The structure and function of communication in society. *The Communication of Ideas*, 1948: 37–52. Retrieved from http://www.dhpescu.org/media/elip/The structure and function of.pdf
21. Walter Lippmann. 1922. *Public Opinion*. Harcourt, Brace and Company, New York, New York, USA.
22. Maxwell McCombs. 2005. A Look at Agenda-setting: past, present and future. *Journalism Studies* 6, 4: 543–557. http://doi.org/10.1080/14616700500250438
23. Maxwell E. McCombs and Donald L. Shaw. 1972. The Agenda-Setting Function of Mass Media. *Public Opinion Quarterly 36*, 176. http://doi.org/10.1086/267990
24. mediaQuant. 2017. Technology Trends. Retrieved from https://www.mediaquant.net/trends-small-mobile-free/
25. M.B. Miles and M. Huberman. 1994. *Qualitative Data Analysis: An Expanded Sourcebook*. Sage Publications, Inc.
26. Amy Mitchell, Jeffrey Gottfried, Michael Barthel, and Elisa Shearer. 2016. *The Modern News Consumer*.
27. Jared Newman. 2013. The Target Credit Card Breach: What You Should Know. *Time*. Retrieved from http://techland.time.com/2013/12/19/the-target-credit-card-breach-what-you-should-know/
28. John Oliver. 2016. Encryption: Last Week Tonight With John Oliver. *Video*.
29. Andrea Peterson. 2014. The Sony Pictures hack, explained. *The Washington Post*.
30. Elissa M. Redmiles, Amelia R. Malone, and Michelle

L. Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. *2016 IEEE Symposium on Security and Privacy (SP)*, IEEE, 272–288. http://doi.org/10.1109/SP.2016.24

31. Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2016. How I Learned to be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, ACM Press, 666–677. http://doi.org/10.1145/2976749.2978307
32. Everett M Rogers and James W Dearing. 1988. Agenda-setting research: Where has it been, where is it going? *Annals of the International Communication Association* 11, 1: 555–594.
33. Yves Rosseel. 2012. lavaan: An R Package for Structural Equation Modeling. *Journal of Statistical Software* 48, 2: 1–36.
34. CNN Staff. 2015. CENTCOM Twitter account hacked, suspended. *CNN*.
35. JM Stanton, P Mastrangelo, KR Stam, and Jeffrey Jolton. 2004. Behavioral Information Security: Two End User Survey Studies of Motivation and Security Practices. *AMCIS*, August: 2–8. Retrieved March 6, 2014 from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.92.2938&rep=rep1&type=pdf
36. Sam Thielman. 2017. Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian*.
37. Daniel Victor. 2015. Security Breach at Toy Maker VTech Includes Data on Children. *The New York Times*. Retrieved from https://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html?mcubz=3
38. Kaveh Waddell. 2016. A Hospital Paralyzed by Hackers. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/
39. Rick Wash. 2010. Folk models of home computer security. *Proc. SOUPS '10*, ACM Press, 1. http://doi.org/10.1145/1837110.1837125
40. David Weaver. 1991. Political Issues and Voter Need for Orientation. In *Agenda Setting. Readings on Media, Public Opinion, and Policymaking*. 131–139.
41. Alma Whitten and J.D. Tygar. 1999. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. *Proc. SSYM'99*, 14–28. Retrieved January 13, 2014 from http://www.usenix.org/events/sec99/full_papers/whitten/whitten.ps
42. Kim Zetter. 2015. Hackers Finally Post Stolen Ashley Madison Data. *Wired*. Retrieved from https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/