Journal of Communication Technology | JoCTEC

Published by the Communication Technology Division of AEJMC

No, you probably don't touch your phone 2,617 times per day: A rationale for the *Journal of Communication Technology*

Dr. Jacob Groshek

Associate Professor of Emerging Media Studies

College of Communication

Boston University

Correspondence:

617-353-6421

jgroshek@bu.edu

Original manuscript accepted for publication in

Journal of Communication Technology

Published by the Communication Technology Division of the Association for Education in Journalism and Mass Communication

No, you probably don't touch your phone 2,617 times per day: A rationale for the *Journal of Communication Technology*

Some statistics reach into popular culture, and they often become benchmarks by which both the general public and media researchers come to know and understand ourselves and our social world. One such statistic is how about two-thirds of people receive "at least some of their news" from social media, which comes from the venerable Pew Research Center (Shearer & Gottfried, 2017) and is cited by many studies attempting to show how important social media is in relation to news. Of course, what is not reported in this instance is that the same report identifies only two-in-ten who report doing so often.

The point here is not to criticize Pew or those that cite that particular finding, but to prod deeper into how we know the things that (we think) we know. Which brings me to the statistic that is being reported now somewhat regularly that "we touch our phones . . . about 2,617 times a day" (Winnick & Zolna, 2016).

As reported, this finding includes the astonished emoji (above) and is from the firm known as dscout (see https://blog.dscout.com/mobile-touches). I've heard this figure mentioned at leading research events by some of the brightest folks working in the field, and, as is sometimes the case, an audience full of similarly smart and motivated scholars express their astonishment, nod, and move on thinking we've all *learned* something. But have we? Do we—experts in the area of digital, social, mobile, and online media—really know what we think we know? I don't know.

When I casually mentioned this figure to my Boston University colleague Jim Cummings over lunch recently, he (politely and rightly) scoffed and did some quick math, suggesting that

the figure of about 2,600 touches would equate to over 100 touches per hour if one were to be awake 24 hours everyday. That impossibility led us to discuss what constituted a ‘touch’ (honestly, I didn’t know) and how that would be humanly possible.

So, like any good social scientist, I started to investigate the claim further. Turns out that dscout considered a ‘touch’ to be every tap, type, swipe and click, gathered via an app. Beyond that, what I found was that it was based on just 94 Android users over a period of 5 days, but as best as I could tell, only two-thirds of those participated all five days. The others participated only 2 to 4 days. This means we are making claims about an entire population based on *just 63 opt-in individuals*.

More than that, when I did some additional simple math, I determined that, based on 18 hours spent awake, the figure of 2,617 touches per day add up to just over 2.4 mobile phone touches per minute. Of every waking minute. Of every day. Generally speaking, I’d say this figure is, as constructed, not impossible but also not very plausible – and that those ‘touches’ might not be meaningful indicators of ‘interaction’ between users or content. So, as I see it, the role of the *Journal of Communication Technology* is to be a space that facilitates discussion and cultivates understanding of the ways in which communication technologies are changing not only media processes and content, but also audiences, institutions, and society at large.

Going back to 2010 when Marcus Messner and Homero Gil de Zuñiga and I started on this adventure to publish our own journal for the Communication Technology Division of AEJMC, it seemed so simple and obvious that we needed another point of entry to tackle challenging problems germane to the field but that had broader implications as well. What can I say other than we were all young, ambitious, and perhaps just a bit too optimistic about what the process of launching a journal would entail? Though it has taken some eight-odd years of bureaucracy and countless hours of effort, and we are more or less published by default of out Boston University and the dedicated support of my research assistants, I am pleased to present

the inaugural issue of *JoCTEC*, and happy to report that the relationship of us three founding editors is still intact, and perhaps even more solidified as a result.

Looking at this inaugural issue in particular, I believe we have articles that address issues of great importance as well as useful research and insights for our audience of scholars working in this area. For example, in our lead article, Dr. James Ivory highlights important approaches to methodological reform in media effects research in relation to communication technology. Along these lines, Dr. Erik Bucy makes an important contribution in terms of calibration, and how that can be managed among researchers working in areas of asymmetric message flows, particularly as this process plays out for the vast majority of what can be considered average users. Dr. Marcia DiStaso then provides some excellent examples of communication challenges in cybersecurity as well as pathways forward. Next, Dr. Richard Shaefer outlines key aspects of the integration between data visualization and the capacity to analyze and understand social trends. Finally, Wasim Ahmed provides an essential overview of tools for doing social media research in the contemporary era that will benefit anyone interested in this area of study.

And, to reiterate from our call for papers, since communication technologies themselves have now come to fulfill a central, social role in virtually all forms of mediated communication, the journal welcomes scholarship from a broad area of inquiry. Provided that the focus pertains to communication technologies, this area of inquiry includes but is not limited to studies of advertising, science, networks, health, politics, history, policy, public relations, management, economics, ethics, minorities, visual communication, and social media.

In addition, as the journal is vitally positioned in a growing international field, it strives to be a home for all theoretical and methodological perspectives. Research that informs debates from comparative empirical perspectives is especially welcome, though more conceptual and theoretical approaches are equally invited. Altogether, systematic and rigorous scholarship of

communication technologies and their impacts from virtually any approach from micro to macro and throughout sub-disciplines will be considered.

It is with great pleasure I put forth this inaugural issue and look forward to growing the *Journal of Communication Technology* further as a collaborative effort with our community of contributors and readers. I am deeply indebted to the authors of this issue as well as the steadfast support of our esteemed editorial board. Thank you all, and please share our open-source publications widely.

If you are already reading through this issue, or have learned of *JoCTEC* through another means, we hope you will consider publishing with us. We offer not only expert review (as signified by our Editorial Board) but also fast turnaround and flexibility with content and format. Any questions, just ask. We will do our best to innovate and accommodate quality work that makes a valuable contribution to this field regardless the format.

We are off, with my profound thanks for your support! I look forward to many future successes with this initiative, and could not do it without the CTEC community.

References

Shearer, E., & Gottfried, J. (2017, September 7). News use across social media platforms. *Pew Research Center*. Retrieved from http://www.journalism.org/2017/09/07/news-use-across-social-media-platforms-2017/

Winnick, M., & Zolna, R. (2016, June 16). Putting a finger on our phone obsession; Mobile touches: A study on humans and their tech. *Dscout*. Retrieved from https://blog.dscout.com/mobile-touches

Journal of Communication Technology | JoCTEC

Published by the Communication Technology Division of AEJMC

With Many Looking to Us for Better Answers, We Must Answer Carefully: A Call for Methodological Reform in Research on Effects of Communication Technology

Dr. James D. Ivory

Associate Professor

Department of Communication

Virginia Tech University

Correspondence:

540-231-6507

jivory@vt.edu

Original manuscript accepted for publication in

Journal of Communication Technology

Published by the Communication Technology Division of the Association for Education in Journalism and Mass Communication

With Many Looking to Us for Better Answers, We Must Answer Carefully: A Call for Methodological Reform in Research on Effects of Communication Technology

Abstract

Among the range of approaches and topic areas encompassed by the broad and interdisciplinary field of communication, research on the effects of communication technology is prominent and long-standing. Given the attention that research on the effects of communication technology receives from the scholars, the public, and policymakers, it is imperative that the accuracy, validity, replicability, and reproducibility of that research is a priority. This essay suggests five points, informed by research related to open science, that the community of researchers studying effects of communication technology might bear in mind to protect and promote the most accurate body of knowledge possible.

Keywords

Media Effects; Communication Technology; Replication; Open Science

---

In the view of pioneering communication scholar Wilbur Schramm (1963), communication research spans its various subfields as a unified endeavor: “There is only communication research. All parts of it are related to all other parts, and the landscape is marked off only by the fact that some scholars are centrally interested in one part, some in another” (p. 5).

Without challenging that wisdom, it can also be noted that the various nebulously defined approaches and topic areas within the field of communication have involved unique

contributions to knowledge. Prominent among these areas is the subfield encompassing research on the effects of communication and media technology. Scholarship dealing with new media technologies has long been a key corner of the communication discipline. Academic interest in the advent of the mass media as a social force was one catalyst for the emergence of communication as an academic field of study, and since the early 20th century the arrival of a given new media technology has been demonstrably tailed by a spate of research investigating that new media technology's social effects (Cantril & Allport, 1935; Wartella & Reeves, 1985).

That pattern holds today, with the potential effects of technologies such as video games and mobile devices drawing interest from scholars, clinicians, parents, policymakers, and the courts (American Psychological Association, 2015; Council on Communications and Media, 2016; Ferguson, 2013; Ivory & Holz Ivory, 2016). With so many sets of eyes on the outcomes of research dealing with the effects of communication technology, the stakes are high. It is imperative that research examining the social effects of new communication technology is based in methodological practices that ensure accurate and valid findings.

Across the universe of social and behavioral research, such accuracy and validity cannot be taken for granted. Perhaps most notably in the fields of psychology and medicine, a "replication crisis" (see Lindsay, 2015; Maxwell, Lau, & Howard, 2015) has mounted in recent years around growing concerns that key findings—and even entire bodies of literature and theoretical frameworks—may be based on research documenting phenomena that cannot be consistently observed (Ioannidis, 2005; Open Science Collaboration, 2015). Several systemic problems in the process of social research are cited as culprits for a body of published knowledge that too often cannot be replicated or reproduced. These problems range from "questionable research practices" that inflate the likelihood of significant findings (Fanelli, 2009; John, Loewenstein, & Prelec, 2012; Martinson, Anderson, & de Vries, 2005) in individual studies

to the “file drawer problem” wherein studies producing null findings tend to be less likely to be published, or even submitted for publication (Rosenberg, 2005; Rosenthal, 1979).

While issues with replicability and reproducibility are, at present, less frequently discussed in communication circles, there is ample evidence that communication research also suffers from systemic inflation of significant findings in its published literature (Matthes et al., 2015; Seaman & Weber, 2015; Vermeulen et al., 2015). Concerns also extend to specific research topics dealing with communication technology, such as the possible effects of video games (Bushman, Gollwitzer, & Cruz, 2015; Elson, Breuer, Scharkow, & Quandt, 2014; Ferguson, 2007; Ivory et al., 2015). Such problems with the validity of research findings in the literature are not, for the most part, the results of intentional fraud or overtly malevolent intent by researchers. As Simmons, Nelson, and Simonsohn (2011) describe motivations behind practices that inflate significance of findings thusly: “This is not driven by a willingness to deceive but by the self-serving interpretation of ambiguity, which enables us to convince ourselves that whichever decisions produced the most publishable outcome must have also been the most appropriate” (p. 1365). Therefore, the “pressure to do whatever is justifiable to compile a set of studies that we can publish” (Simmons et al., 2011, p. 1365) is a symptom of a research practice culture that needs to have some of its norms adjusted rather than of sporadic bad acts in the community.

Given the importance of research on effects of communication technology to the field and to a broader audience and given that systemic issues in the production of social research are a legitimate threat to the validity of that research, this article offers a call for some minor methodological reforms to protect and promote the accuracy and validity of research dealing with effects of communication technology. This call takes the form of five simple points addressed to researchers, reviewers, editors, and others in the scholarly community studying

effects of communication technology regarding ways that our research culture can be as conducive as possible to production of accurate, valid, replicable, and reproducible knowledge.

Five Suggestions for Future Research on Communication Technology Effects

1. Nothing is Something: Null Findings Teach Us About Communication Technology Effects, Too

The "media effects" approach to communication has been a dominant perspective in both communication technology research and the broader communication field (Eveland, 2003), but the approach may, down to its very name, also be inadvertently plagued by a bias toward research finding such effects. Given that the "file drawer" problem is prominent across social research (Rosenberg, 2005; Rosenthal, 1979), scholars interested in effects of communication technology must be especially mindful of avoiding publication bias—a broad preference for significant findings at all levels of the research process that cumulatively produces an inflated appearance of media effects in the literature.

Sometimes, media technologies have a noteworthy effect on outcomes in our lives. Sometimes, they do not. To ensure that the entire spectrum of communication technology effects—including null effects—is included in the record of knowledge, we must be mindful of the need to avoid privileging significant findings when we conduct our own research and when we evaluate the research of others. The latter is particularly important, as authors who might otherwise be comfortable with reporting and submitting null findings may be less so when discouraged by reviewers and editors. Feedback along the lines of "This was a great study idea; it's a pity the results weren't significant" must become a thing of a past if we are to be sure that our research is focused on the quality of the questions we ask about communication technology and the methods we devise to answer them rather than on the answers we get.

2. Context is Everything: Baseline Comparisons Inform Findings about Communication Technology Effects

While learning to embrace null findings may be one ongoing challenge for scholars, a similar challenge deals less with the presence of effects than with the magnitude of them. Reporting statistical effect sizes is an increasingly common practice in communication research, even a prerequisite for publication. Such statistics provide information about the strength of association between variables, which is useful context. In the specific research area of effects of communication technology, another useful indicator of magnitude is information about how effects of the specific technology of interest compare to effects of alternative technologies or activities. Indeed, a communication technology may have a measurable effect on an outcome, but the societal importance of that effect may be in its magnitude relative to the technology's alternatives. Providing such comparisons, both in formal research reports and in popular media outreach such as press releases, would do much to discourage misinterpretation of an observed effect's novel impact on individuals and society.

An outstanding example of the value of such comparisons can be found in a recent study by Przybylski and Weinstein (2017), who report some associations between high amounts of weekday digital screen time and problems with mental well-being among a large sample of British adolescents. They carefully qualify the urgency of their findings, though, by noting that the strength of association between screen time and well-being in their study was much smaller in magnitude than associations between well-being and breakfast or sleep habits. Such comparisons provide an excellent opportunity to contextualize the impact of communication technology on our lives rather than promote all observed effects as substantially detrimental or beneficial to the lives of users.

3. Show Our Work: Reducing Methodological Flexibility Will Ensure Valid Findings about Communication Technology Effects

The importance of encouraging reportage and publication of null effects (as well as contextualizing the magnitude of observed effects) has already been discussed here. However, the incentive to produce research showing effects of communication technology is not eliminated by merely increasing publication of null findings. Researchers may be predisposed to findings that support an existing theoretical framework, a previous program of research, or simply an exciting finding. Without ill intent, a researcher may increase the likelihood of significant findings by incorporating "researcher degrees of freedom" (Simmons et al., 2011) in a study design, providing more opportunities to produce a desired outcome. Choosing which cases to remove, how to compute an outcome measure, which variables to include in a statistical model, which measures to report, and a host of other decisions all introduce a "garden of forking paths" in which a study can inadvertently provide scores of potential outcomes to compare in search of a preferred finding (Gelman & Loken, 2014). Even without deliberately "p-hacking" to produce a desired significant result, a researcher motivated to expect a certain effect might consequently report significant patterns picked from noise in a data set. This selectivity is perhaps a particular concern with measures that are designed to allow flexible use (see Elson et al., 2014).

A remedy for such inflation of significant effects is transparency and *a priori* decision-making throughout the research process. Providing open access to data sets via freely available services (including notably the Open Science Framework; http://osf.io) allows specific analyses to be reproduced but also allows alternate analyses to be conducted to be sure a finding is not the product of a delicate combination of analysis decisions rather than a robust effect of the technology under study. Further, an array of tools (one of many examples is As Predicted; http://aspredicted.org) allow pre-registration of study designs and analysis plans to ensure careful consideration of a conceptually appropriate methodological strategy in advance rather than *post hoc* decisions made from among a smorgasbord of reportable findings (Nosek &

Lakens, 2014). With a broad audience interested in what researchers learn about communication technology effects, sharing access to how that knowledge was produced adds substantially to its credibility. Authors can use these tools to increase the credibility of their findings, while reviewers and editors can encourage such open practices to increase their confidence in the studies they evaluate.

4. Demolition Allows Development: Letting Go of Findings that Do Not Replicate Ensures Accurate Knowledge about Communication Technology Effects

If we achieve a research environment where a broader range of results are reported and published, and where studies have less flexibility in analyses to produce outcomes that may be preferable, then that environment is one where our research findings are more accurate. Unfortunately, though, such an environment can also be one where popular findings and theories from the previous, more flexible, and more effects-friendly research climate are not well-supported. In behavioral science, replication initiatives commonly fail to support some previously celebrated findings (Open Science Collaboration, 2015). Previous findings may have been inflated by biases in the research process, or they may be flukes of chance rather than consistently observable phenomena (Ioannidis, 2005).

In any case, there will be instances where authors, reviewers, and editors encounter results that challenge popular scholarly beliefs about effects of technology. Such challenges must be welcomed by authors as well as by editors and reviewers. Lewin's (1952) maxim, "There is nothing more practical than a good theory" (p. 169) may ring true, but a theory loses its practicality when evidence no longer consistently supports it as presented. Articles published in major communication journals display an increased proliferation of proposed theories (Anderson, 2016); culling them based on evidence will allow the strongest frameworks to flourish. As we conduct and evaluate research, we must maintain a healthy receptiveness toward falsification of our assumed knowledge.

5. If Being Wrong is Wrong, I Do Not Want to Be Right: Acknowledging and Embracing Errors and Limitations in Our Past Research is a Noble Contribution to Knowledge

Finally, if we will find sometimes that previous research has been wrong, then we may find sometimes that *our own* previous research has been wrong. This realization will not likely be pleasant. A researcher may have invested considerable effort into a program of research, and it may be difficult to countenance a lack of support from new data. Further, a researcher may have produced findings using accepted strategies at the time but later realize in a changed research environment that those strategies inflated the significance of findings and are now discouraged. In both situations, there may be feared impacts on reputation, and even careers.

Here, it is crucial that we are responsible with the uncomfortable outcomes of new research culture. If we are indeed able to produce a climate in research on communication technology effects where we see more common publication of null findings, more clarity about the comparative context of effects, more transparency and less flexibility in analyses, and more falsification of prior research, then we need to consider implications for the people involved—ourselves and others—carefully. While some practices, such as demonstrable fraud, should have negative consequences for researchers, findings that are simply falsified by improvements in research practice should not be viewed as a source of shame so much as proverbial "products of their time."

An author acknowledging that a prior finding is no longer one that can be interpreted confidently is not only candid; that author is voluntarily accelerating correction of the scientific record. Thus, we need to take an "amnesty" approach when hindsight allows a researcher to see limitations in a study and congratulate the nobility of righting past errors. A crucial part of improving the norms of research practice, then, is for the community of researchers interested in communication technology effects to welcome—and even applaud—self-inspection and self-correction of the research record.

Conclusions and a Final Call

I expect to enjoy observing a future of innovative programs of research conducted by brilliant, hard-working, and well-intended researchers. This article aims to suggest how we can all help each other ensure that the future is also one where we can be more confident in the knowledge we produce. While one touted hallmark of science is that it is self-correcting, it is folly to assume that a research field will self-correct without eradication of systemic biases against self-correction (Ioannidis, 2012). Researchers studying effects of communication technology are trusted by many for guidance about the new devices, media content, and interactions that continue to flood into their lives. We must honor that trust by ensuring that our research community's norms and standards ensure the most accurate body of knowledge possible.

References

American Psychological Association. (2015). *Resolution on violent video games.* Retrieved from http://www.apa.org/about/policy/violent-video-games.aspx

Anderson, J. A. (2016). Communication descending. *International Communication Gazette.* (Online First Publication). doi:10.1177/1748048516655708

Bushman, B. J., Gollwitzer, M., & Cruz, C. (2015). There is broad consensus: Media researchers agree that violent media increase aggression in children, and pediatricians and parents concur. *Psychology of Popular Media Culture, 4,* 200–214. doi:10.1037/ppm0000046

Cantril, H., & Allport, G. W. (1935). *The psychology of radio.* New York: Harper.

Council on Communications and Media. (2016). Media and young minds. *Pediatrics, 138,* e20162591. doi:10.1542/peds.2016-2591

Elson, M., Mohseni, M. R., Breuer, J., Scharkow, M., & Quandt, T. (2014). Press CRTT to measure aggressive behavior: The unstandardized use of the competitive reaction time

task in aggression research. *Psychological Assessment, 26,* 419–432. doi:10.1037/a0035569

Eveland, W. P., Jr. (2003). A “mix of attributes” approach to the study of media effects and new communication technologies. *Journal of Communication, 53,* 395–410. doi:10.1111/j.1460-2466.2003.tb02598.x

Fanelli, D. (2009). How many scientists fabricate and falsify research? A systematic review and meta-analysis of survey data. *PLoS One, 4*(5)*,* e5738. doi:10.1371/journal.pone.0005738

Ferguson, C. J. (2007). Evidence for publication bias in video game violence effects literature: A meta-analytic review. *Aggression and Violent Behavior, 12,* 470–482. doi:10.1016/j.avb.2007.01.001

Ferguson, C. J. (2013). Violent video games and the Supreme Court: Lessons for the scientific community in the wake of *Brown v. Entertainment Merchants Association. American Psychologist, 68,* 57–74. doi:10.1037/a0030597

Gelman, A., & Loken, E. (2014). The statistical crisis in science. *American Scientist, 102,* 460–465.

Ioannidis, J. P. A. (2005). Why most published research findings are false. *PLoS Medicine, 2*(8)*,* e24. doi:10.1371/journal.pmed.0020124

Ioannidis, J. P. A. (2012). Why science is not necessarily self-correcting. *Perspectives on Psychological Science, 7,* 645–654. doi:10.1177/1745691612464056

Ivory, J. D., & Holz Ivory, A. (2016). Playing around with causes of violent crime: Violent video games as a diversion from the policy challenges involved in understanding and reducing violent crime. In S. Conway & J. DeWinter (Eds.), *Video game policy: Production, distribution, and consumption* (pp. 146–160). New York: Routledge.

Ivory, J. D., Markey, P. M., Elson, M., Colwell, J., Ferguson, C. J., Griffiths, M. D., . . . Williams, K. D. (2015). Manufacturing consensus in a diverse field of scholarly opinions: A comment on Bushman, Gollwitzer, and Cruz (2015). *Psychology of Popular Media Culture, 4,* 222–229. doi:10.1037/ppm0000056

John, L. K., Loewenstein, G., & Prelec, D. (2012). Measuring the prevalence of questionable research practices with incentives for truth telling. *Psychological Science, 23,* 524–532. doi:10.1177/0956797611430953

Lewin, K. (1952). *Field theory in social science: Selected theoretical papers by Kurt Lewin.* London: Tavistock.

Lindsay, D. S. (2015). Replication in psychological science. *Psychological Science, 26,* 1827–1832. doi:10.1177/0956797615616374

Martinson, B. C., Anderson, M. S., & de Vries, R. (2005). Scientists behaving badly. *Nature, 435,* 737–738. doi:10.1038/435737a

Matthes, J., Marquart, F., Naderer, B., Arendt, F., Schmuck, D., & Adam, K. (2015). Questionable research practices in experimental communication research: A systematic analysis from 1980 to 2013. *Communication Methods and Measures, 9,* 193–207. doi:10.1080/19312458.2015.1096334

Maxwell, S. E., Lau, M. Y., & Howard, G. S. (2015). Is psychology suffering from a replication crisis? What does “failure to replicate” really mean? *American Psychologist, 70,* 487–498. doi:10.1037/a0039400

Nosek, B. A., & Lakens, D. (2014). Registered reports: A method to increase the credibility of published results. *Social Psychology, 45,* 137–141. doi:10.1027/1864-9335/a000192

Open Science Collaboration. (2015). Estimating the reproducibility of psychological science. *Science, 349*(6251)*,* aac4716. doi:10.1126/science.aac4716

Przybylski, A., & Weinstein, N. (2015). A large-scale test of the Goldilocks hypothesis: Quantifying the relations between digital-screen use and the mental well-being of adolescents. *Psychological Science.* (Online First Publication). doi:10.1177/0956797616678438

Rosenberg, M. S. (2005). The file-drawer problem revisited: A general weighted method for calculating fail-safe numbers in meta-analysis. *Evolution, 59,* 464–468. doi:10.1554/04-602

Rosenthal, R. (1979). The file drawer problem and tolerance for null results. *Psychological Bulletin, 86,* 638–641. doi:10.1037/0033-2909.86.3.638

Seaman, C. S., & Weber, R. (2015). Undisclosed flexibility in computing and reporting structural equation models in communication science. *Communication Methods and Measures, 9,* 208–232. doi:10.1080/19312458.2015.1096329

Schramm, W. (1963). Communication research in the United States. In W. Schramm (Ed.), *The science of human communication* (pp. 1–16). New York: Basic Books.

Simmons, J. P., Nelson, L. D., Simonsohn, U. (2011). False-positive psychology: Undisclosed flexibility in data collection and analysis allows presenting anything as significant. *Psychological Science, 22,* 1359–1366. doi:10.1177/0956797611417632

Vermeulen, I., Beukeboom, C. J., Batenburg, A., Avramiea, A., Stoyanov, D., van de Velde, B., & Oegema, D. (2015). Blinded by the light: How a focus on statistical “significance” may cause *p*-value misreporting and an excess of *p*-values just below .05 in communication science. *Communication Methods and Measures, 9,* 253–279. 10.1080/19312458.2015.1096333

Wartella, E., & Reeves, B. (1985). Historical trends in research on children and the media: 1900–1960. *Journal of Communication, 35,* 118–133. doi:10.1111/j.1460-2466.1985.tb02238.x

Journal of Communication Technology | JoCTEC

Published by the Communication Technology Division of AEJMC

The Calibration Problem: ICT Complexity and Average User Competencies

Erik P. Bucy

Marshall and Sharleen Formby Regents Professor of Strategic Communication

College of Media and Communication

Texas Tech University

Correspondence:

806-834-3346

erik.bucy@ttu.edu

Original manuscript accepted for publication in

Journal of Communication Technology

Published by the Communication Technology Division of the Association for Education in Journalism and Mass Communication

The Calibration Problem: ICT Complexity and Average User Competencies

When the World Wide Web opened the networked infrastructure of the Internet to use on a large scale, much hope was pinned on the new medium's potential to evolve into an "information superhighway" where an endless array of facts would be at the public's beck and call for edification and self-enlightenment. Visionary technologists had imagined similar systems decades earlier—"wholly new forms of encyclopedias . . . ready made with a mesh of associative trails running through them," as Vannevar Bush (1945, para. 65) described his Memex concept. Much popular speculation also focused on the politically empowering role of information and communication technologies (ICTs) to serve as organizing agents for social change (Grossman, 1995; Rheingold, 2002). Although, some did warn about the "disappointing realities" of online message flows, including their susceptibility to spreading rumor and valorizing trivia, to lending credibility to extreme opinions, and to circulating false information at cybernetic speeds (Stoll, 1995, pp. 218-224).

At the same time, researchers have documented the numerous challenges facing individual users in complex information environments that argue against the view of ICTs as a liberating and rationalizing force in society (see Bucy & Newhagen, 2004; van Dijk, 2005, 2012). First, effective use of ICTs for social, educational, and political action requires not only physical access to digital technologies and motivation to use them but a succession of skills that include operational, informational, and strategic abilities to leverage network capacities. The ability to search, process, and utilize information in complex digital spaces "cannot be taken for granted," van Dijk (2005, p. 73) cautioned. "These skills have to be learned" (van Dijk, 2005, p. 73).

Typical user orientations toward information and communication technologies, however, suggest that motivation to learn is limited. Surveys of baseline digital skills of even "universally wired" groups of Internet users show considerable variation in user competence, number of network access points, time spent online, and self-assessed ability (Hargittai, 2010). Digital

skills are also lower for less privileged segments of society, and lower perceived skill significantly affects online behavior and types of uses to which less skilled users will put the medium (Hargittai & Shafer, 2006).

Key to understanding the nature of these challenges is the level of analysis at which arguments about technological influences are made. In the case of political empowerment, a broad perspective is often embraced that reflects a social level of analysis, where technology seems to enable collective movements to achieve desired ends—even if such success means primarily delivering on a sense of shared community (see Papacharissi, 2015). Castells (2007, 2009) cites the advent of several trends, including Internet-based fundraising and mobilization, organizing via mobile media, and the appearance of autonomous communication networks supported by the Internet and wireless communication not under the control of dominant media players as evidence of a new phase of counter-power in the network society. Bennett (2013) further examines the organization of power in communication-based networks, showing how the logic of "connective action" is coordinated using inclusive discourses, such as the "We Are the 99%" slogan that traveled through social media during the Occupy Wall Street protests.[1]

When describing successful collective action efforts enabled by technology, mobilization enthusiasts are largely extolling the sociology of mass movements. In effect, they are documenting the achievements of a new class of information elites—activists who harness the democratizing potential of technology to devise workarounds to entrenched power structures; they are not, however, describing the abilities or inclinations of average users. Average, or end, users now more often serve as targets of online communication campaigns, particularly on social media, than they do as original content providers or political organizers. As observed elsewhere (Bucy & Zelenkauskaite, 2014; Zelenkauskaite & Bucy, 2016), the growing capacity of networked systems to track, collate, and parse online behaviors exercises power over and discriminates against average users by extracting their data for marketing purposes (typically without their full consent and understanding) and then bombarding them with tailored

advertising and unsoliticed persuasive messaging. The quality of message flows for the average user in the networked environment is one of besieged inundation rather than liberating autonomy.

Asymmetric message flows

Nowhere was this concept more apparent than during the 2016 U.S. presidential election, where the onslaught of dubious information sources, fake news reports, and bot-generated content on social media platforms—dubbed "computational propaganda" (see Markoff, 2016)—taxed the ability of even dedicated fact-checkers (Dale, 2016).[2] This unprecedented situation presented a problem familiar to psychologists who have studied information acceptance. First, most citizens could not contend with the pace and volume of political information that would go viral—it is far easier to just click on or forward a piece of outrageous or salacious information than to verify its authenticity first, particularly if that story reinforces a stereotype. Hence, a Buzzfeed analysis found during the General Election that the 20 top-performing *false* election stories from hoax sites and hyperpartisan blogs (e.g., "Just Read the Law: Hillary Is Disqualified From Holding Any Federal Office") generated 1.3 million more shares, reactions, and comments on Facebook than the 20 best-performing legitimate election stories from major news websites—8.7 million compared to 7.4 million (Silverman, 2016).

Second, even if an effort was made to verify suspect content, there is a psychological tendency grounded in evolutionary theory to accept initial claims as true *first* before then deciding to reject them (Gilbert, Krull, & Malone, 1990), so the initial acceptance of bogus information often wins out over well-intentioned but insufficient efforts to correct false claims.

Against this backdrop of asymmetrical information flows—flows that represent the exercise of network power—the average user is increasingly defenseless to turn back the information tide and exercise a meaningful degree of control over the quality of their news

intake. The inability of users is paradoxical because interactive media are supposed to give users *more* control over their media experiences. In many ways they do, enabling customized browsing sessions and enhancing entertainment experiences especially (Kalyanaraman & Wojdynski, 2015). However, this base-case scenario does not present when it comes to news, where interface affordances may give users a sense of feeling closer to newsworthy developments but often leave them feeling confused (Bucy, 2004). Engaging in "second screen" activity through a mobile device, as when viewers of presidential debates tweet to other viewers in real time, may enhance a sense of participation, but multitasking typically comes with the cognitive cost of not retaining much information (Ophir, Nass, & Wagner, 2009). As a result, users have difficulty navigating complex digital environments and sorting out fact from opinion—even seeing more risk if reader comments *underneath* an online news story are infused with enough incivility or negativity (Anderson, Brossard, Scheufele, Xenos, & Ladwig, 2013).

This pollution of the information environment, increasingly planned by strategic actors operating in the policy sphere with the goal of diffusing dissent, undermining science claims, casting doubt on established facts, or influencing elections (Markoff, 2016; Wertime, 2016), is not limited to online media either. The totality of opinion journalism, whether on cable "news" networks, partisan blogs, or talk radio, traffics in a similar politics of assertion and confrontation over reason (see Mutz, 2015).

In the pre-cybernetic and pre-opinion news era (roughly, the time prior to the rise of the World Wide Web, conservative talk radio, and the Fox News Channel),[3] media personnel involved in producing the printed newspaper and daily newscast made editorial decisions on behalf of audiences and insulated everyday citizens from having to search for and verify important developments themselves. Granted, this coverage was not always as enterprising or hard-hitting as it might have been (Fallows, 1996; Hertsgaard, 1989), but surveillance and correlation of different elements of society were among the news media's major acknowledged functions (Lasswell, 1948) and few questioned the central role of the press in providing "a

complete and honest account of the day's events." As digital media have supplanted the printed press and the universe of television content has exploded, that burden of surveillance—of information search, curation, and verification—has largely devolved onto the individual, who must now navigate an expanding universe of content choices and delivery platforms, deciding what is important, believable, and true and what is not.[4]

Thus, social level, and largely anecdotal, arguments about power redistribution through networked media are seriously challenged when brought down to the level of the individual user, where skill deficiencies, lack of training, usage gaps, uneven motivation, and other barriers to full media access prevail (van Dijk, 2005; see also Hargittai, 2010; Hargittai & Shafer, 2006; Newhagen & Bucy, 2004). Unlike earlier analog media, which demanded a more straightforward (though nontrivial) kind of user expertise—reading in the case of newspapers, the ability to parse oral communication in the case of radio, visual acumen and an appreciation for dialog and drama in the case of television or film—a wide range of cognitive and technical abilities must be brought to bear to successfully navigate networked spaces and make gainful use of online resources. In study after study, the average user does not display the high degree of information efficacy, political interest, or technical ability that network mobilization advocates assume. If you are not an activist offline, you are unlikely to become one online.

Indeed, users are empowered to make full use of new communication technology only to the extent that they are cognitively, motivationally, and technically able. Even assuming motivation, the cognitive and technical barriers to full media access are considerable. Unlike television, the interconnected, multimodal, and software-dependent quality of networked communication technologies—their integrative or *remedial* properties, in the phrase of Bolter and Grusin (2000)—makes online media strikingly different from earlier, analog platforms in their degree of complexity. This complexity derives from the layered quality of network architecture, high degree of system adaptability by means of computer software, and unique affordances of different digital platforms. Together, networked media are characterized by

distinct system functions, multiple traffic patterns or information flows, communication at different levels of analysis, and—through a proliferating number of digital devices—growing interface variation.

Contrasting configurations of communication

This veritable collision of qualities not surprisingly produces multiplicative and contrasting configurations of communication and interaction, a $4 \times 4 \times 4 \times 4$ conceptual matrix that remains beyond the reach of the average user to fully comprehend and leverage. Imagine here the difficulty of solving a Rubik's cube, only the challenge is not sequential and cannot be solved with a simple algorithm. First, communication even without technology can occur at four different *levels of meaning*: interpersonal, group, organizational, and mass. Through different applications and platform interfaces, the Web accommodates each of these levels, for example, through email, chat, teleconferencing, social media apps, company or department intranets, and mass media websites. Adding to the complexity, all four levels of communication can occur simultaneously on the same screen, depending on which application windows are open.

Thus, in the networked environment we start out with four levels of communication (4×1). But the Web, as a computationally based system, is capable of much more than communication. As December (1997) pointed out early in the networked era, the Web as a technological system facilitates at least four *basic functions*: communication, information exchange, interaction, and computation. Communication, which involves the exchange of meaning through the use of symbols or nonverbal signals between two or more people through the network, differs from information exchange, which is the dissemination and retrieval of stored data or knowledge. Interaction entails uses of the network for reciprocal exchanges aside from information, such as game play, activities in virtual worlds, or group interactions. Computation involves data processing, which the Web, even though we now think of it as a

communication platform, still performs quite handily. Each function represents a distinct class of activity that, when combined together on a single distributed platform, endows the distributed network of servers supporting the Web more versatility and processing capacity than all other media platforms combined.

Crossing levels of communication with functions of the networked environment produces 16 unique information and communication configurations (4×4).

Within these contrasting levels of communication, interactional dynamics, and system functions, information and data traffic may flow in at least four distinct directions, as detailed by Bordewijk and van Kaam (1986) in their seminal discussion of information traffic patterns in tele-information services. In their typology of data flows, they distinguish between four different patterns of exchange. The first, allocution, models a transmission process from a service center to an individual consumer or locality; this is the network's capacity to "push" content to users based on inputted preferences or collaborative filtering that determines your preferences based on transaction log data. Mostly, it represents a one-way flow of messages to the end user, combining "many of the traits of networks with those of broadcast" (Kelly & Wolf, 1997, para. 11), Consultation, the inverse of allocation, reflects a dynamic where the service center only delivers information at the specific request of the consumer, as with queries to search engines, online encyclopedias, or medical reference sites. "Consultation requires more activity by the consumer than allocution, but also grants much more freedom in selecting the information required" (Bordewijk & van Kaam, 1986, p. 577).

Perhaps the most troubling, and insidious, traffic pattern is registration, where the service center "no longer has the task of issuing information, but of collecting it" (Bordewijk & van Kaam, 1986, pp. 579–580). At the most basic level, networked systems require users to establish log-in protocols and passwords before gaining access to services and increasingly require users to complete extensive credit type applications to gain full use, as with Apple's much reviled iTunes platform. In the process of using the service, or posting content to social

media communities, user-generated content is captured as a matter of routine so that consumers can then be advertised to more efficiently. Even with simple Web browsing, cookies track user movements and compile browsing and purchasing histories that have utility to advertisers. Although recognized early on and heavily criticized as a practice (see Garfinkel, 2000; Rosen, 2001), extracting information from users in the process of providing services has become the primary function of most network destinations today.

The fourth traffic pattern, conversation, represents peer-to-peer communication where information-handling capacities are divided equally between two terminals, as with email, voice over Internet protocol (VoIP), chat or other short messaging services. Thus, varying traffic patterns add another layer of complexity onto networked media. Crossing levels of communication with functions of the networked environment and now information traffic patterns produces 64 unique information and communication configurations ($4 \times 4 \times 4$).

Finally, each of these contrasting communication and information configurations, with their varying interactional dynamics, system functions, and data traffic flows, may be accessed and transacted over different *hardware platforms*, including desktop and laptop computers, tablet devices, and Internet-enabled mobile phones. The distinction here may seem trivial—interfaces mostly differ in size, right?—until consideration is given to the unique set of technical skills required to put each new device to strategic use, the demands of software upgrades and new models of use like “cloud computing,” and the digital dexterity required to work seamlessly across the idiosyncrasies of screens large and small (not to mention differences and incompatibilities between Windows, Mac, and Android operating systems).

Crossing levels of communication with functions of the networked environment, information traffic patterns and, now, different hardware platforms through which users access and interact with content and other users produces 256 unique information and communication configurations ($4 \times 4 \times 4 \times 4$).

Hardware requirements constantly change and advance as well, requiring continuous investment in the means of physical access to take full advantage of system offerings. Hand a smart phone to a flip phone user and the device will seem exotic and inaccessible, barely resembling a phone at all. Updates and system design changes are now so routine and frequent that computer instruction manuals have become a quaint artifact of a bygone era—users must now teach *themselves* how the system operates and become autodidactic in their approach to technology. Self-learning provides a workable solution for some, but not all, users and turns the discussion about media access toward the question of motivation.

Media access and motivation

In *Media Access: Social and Psychological Dimensions of New Technology Use*, Bucy and Newhagen (2004) catalogued the skills, motivations, and psychological resources that audiences, whether conceived as citizens or consumers, must possess to strategically utilize new communication technologies. The old assumption, particularly concerning networked media adoption, was that physical access to computer hardware and telecommunications infrastructure was sufficient to resolve disparities in use. From a media access perspective, the problem instead needs to be considered in much broader human and technological terms. Importantly, a distinction needs to be made between having physical access to the Internet—or any networked medium—as a *technology* and being able to cognitively access and process the *content* that resides on it. Because of the multimodal character of content online—namely, the simultaneous interaction of text and images in a layered system that accommodates myriad contrasting configurations of communication and information traffic flows—"a broader range of psychological processes will have to be considered than has been the case for traditional mass media" (Newhagen & Bucy, 2004, p. 13).

Using this observation as a departure point, next generation technology research should more explicitly take user skills into account as moderators of effects—not just to estimate

computer expertise in the population but to investigate *how* expertise shapes and delimits online experiences. Research on videogame play, for instance, has shown that skill level not only determines how far users progress in gameplay but how much of the game world their characters see and amount of violence they encounter (Matthews & Weaver, 2013). Higher skilled players perpetrate violence more often than lower skilled users, while lower skilled users more often suffer as the targets of violence—and express more frustration after game play (Nowak, Krcmar, & Farrar, 2008). This frustration, the authors surmise, could either stem from repeated victimization within the game *or* having to learn the game mechanics, which together could cause disorientation and confusion, along with hostility toward the game environment. These results seem highly applicable and could serve as a metaphor for the broader experience of online search and content navigation more generally.

Skill level not only defines and circumscribes the experiences of users within digital environments, but it may also affect motivation to engage with technology in the first place. The social context of technology use, often overlooked in studies of usage gaps and digital divides, is another important consideration. Socioeconomic class, life circumstances, community infrastructure, and even expectations within families form a more durable and persistent class outlook toward ICTs than commonly assumed (Rojas, Straubhaar, Roychowdhury, & Okur, 2004). Appropriating Bourdieu's notion of *habitus* or "dispositions that create durable and transposable practices and perceptions over a long process of social inculcation," Rojas and colleagues (2004, p. 114) identify a shared understanding or orientation toward technology ("technodisposition") that prevents young users in downtrodden communities from engaging with information technologies in ways that are personally empowering or useful. Despite such conventional remedies as free wifi, low-cost computing, wired schools and libraries, and other public access centers, facilitating *social access* to networked systems remains a daunting challenge.

Some point to smartphone technology as the workaround to the thorny issues associated with full media access, or as it has been called in the human-computer interaction literature, *universal usability* (Shneiderman, 2000). In early 2015, *Wired* magazine pronounced that, “In less than two years, a smartphone could be your only computer” (Bonnington, 2015). Granted, in terms of convenience and versatility, there is a case to be made for the smartphone as a technology capable of “leapfrogging” the traditional computing platforms of desktops and laptops—particularly for social and entertainment needs. But even as new ways are found for the smartphone to facilitate communication and interface with other playback devices, their informational and computational power remains limited.

Settling for a mobile device over a true computing platform entails a tradeoff between convenience and power, a tradeoff that reinforces the average user’s *end user* status. While their storage and processing capacities of mobile devices are growing, they are nowhere near as robust as full-size platforms and have far fewer capabilities. Although terminal emulators running on iOS and Android devices now make it possible to access mainframe systems remotely, the reduced memory and processing speeds of mobile compared to desktop devices compromises smartphones as input/output devices, making them difficult to work with on anything except smaller projects and files. Apps and mobile operating systems are similarly anemic compared to the fully featured operating systems and programs found on computers. “The handheld smartphone is a gutless wonder compared with the desktop machine,” computer guru John Dvorak (2012, para. 2) declared a few years ago. “What we have is a touch-screen phone that has cloud access and can run some rudimentary code called ‘apps.’”

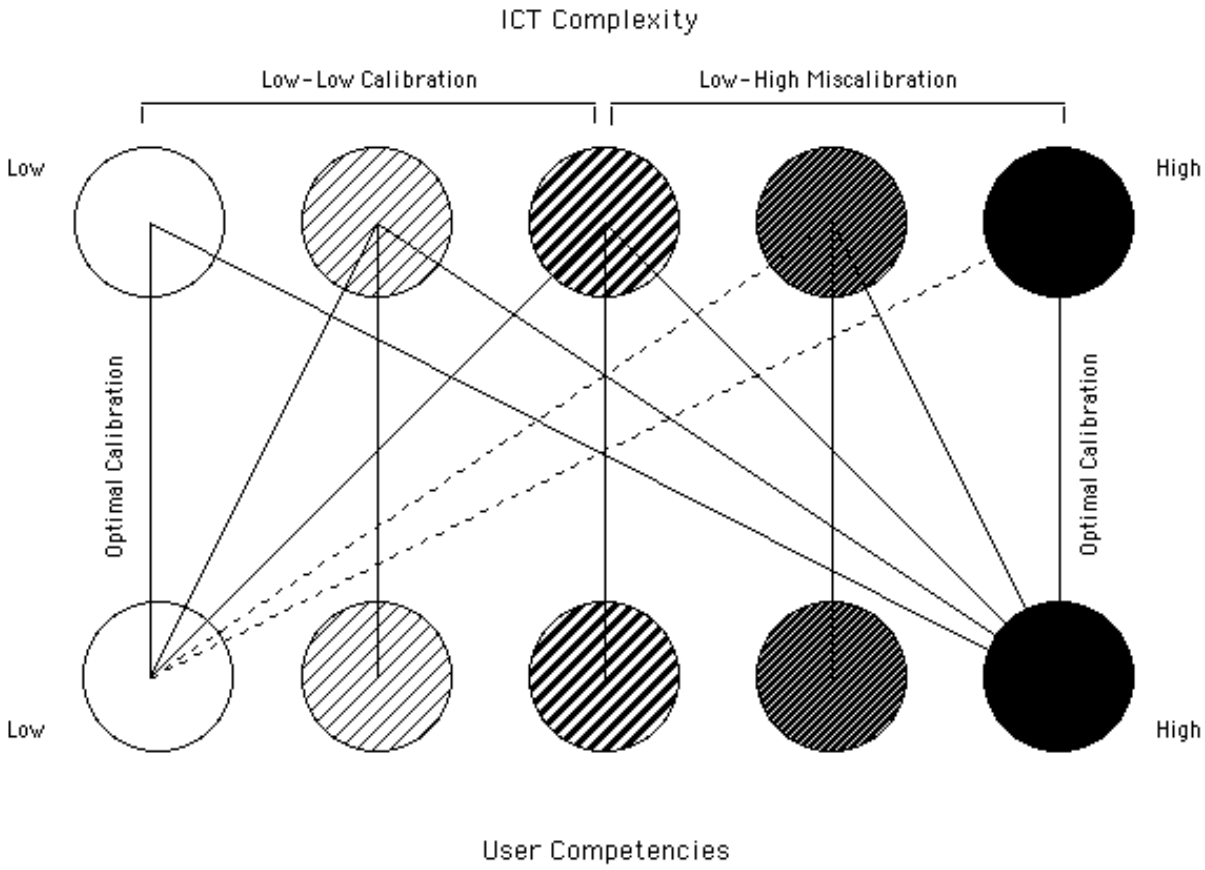
Granted, the smartphone of 2018 (e.g., Apple’s iPhone X) is much more advanced than the smartphone of 2012 (e.g., the iPhone 5)—but so are the latest desktop and laptop computers. For the foreseeable future, then, computers will continue to run the technology table, presenting the familiar barriers to full media access.

User-to-system calibration

A critical but often overlooked factor influencing whether users are positioned to make gainful use of interactive media is the degree to which their skills, motivations, and competencies are properly *calibrated* or congruent with the challenges presented by the medium (Hoffman & Novak, 1996). Calibration is a particularly vexing problem with networked computing, which confronts the user with communication opportunities at a wide range of levels (from interpersonal to mass), across different devices, while encountering varying traffic patterns and interface demands. Online, the user enters a cognitively demanding setting marked by many different and contrasting configurations of communication (Morris & Ogan, 1996; Newhagen & Bucy, 2004).

Figure 1 illustrates how users with a high level of competency (the darkest circles along the bottom row) possess the skills necessary to benefit from just about any degree of ICT complexity. The vertical lines to the top row represent optimal calibration, while the solid angled lines represent adequate calibration or, at worst, a *skills surplus*. Sophisticated users are equipped to effectively engage with the most to the least complex technologies. However, low-end users (the lightest circles along the bottom row) have considerably less flexibility. As the diagram indicates, low-end users are able to take advantage of interactive media as long as the degree of complexity remains moderate. As the complexity level increases, a threshold is crossed and a miscalibration or *skills deficit* occurs (represented by the dashed angled lines). In this situation, low-end uses have the option of either improving their skills and meeting the technology at the required level of expertise or (perhaps more likely) abandoning their efforts altogether after a period of initial, frustrating use (see Bessiere, Ceaparu, Lazar, Robinson, & Shneiderman, 2004).

Figure 1: The calibration problem. Illustration of the degree to which user skills, motivations, and competencies may be (in)congruent with system demands.



The flip side of the calibration problem is that sophisticated users, in the case of a skills surplus, may not feel sufficiently challenged by noninteractive media to give it their ongoing attention. As Hoffman and Novak (1996) comment in relation to computer-mediated environments (CMEs), “if network navigation . . . does not provide for congruence of skills and challenges, then consumers either become bored (i.e., their skills exceed the challenges) or anxious (i.e., the challenges exceed their skills) and either exit the CME or select a more (or less) challenging activity within it” (p. 60). Anecdotally, the popularity of interactive and participatory media, particularly among younger users, suggests that audience segments

accustomed to interactive experiences come to expect a certain level of hands-on engagement and create it for themselves when it cannot be found in one medium alone (Jenkins, 2008). The resulting fracturing of attention has, according to media critics, caused content producers to create faster-paced, more visually oriented productions with a fragmented story structure intended to stave off restlessness (Gleick, 2000).[5] Thus, the calibration problem associated with interactive media has implications for both sophisticated and unsophisticated users alike.

As this discussion of calibration issues suggests, future research into network technology effects should consider the ratio of user skills, motivations, and competencies to system challenges. Research should not be satisfied with merely identifying *when* a networked communication setting is perceived as challenging (although more work needs to be done in this area) but should also ultimately address the *consequences* of skills deficits, skills surpluses, and varying barriers to full media access.

In the case of an enduring miscalibration between user skills and system challenges, for example, the interactive technology may prevail and alienate average users from the Web's social and informational bounty.[6] In his account of the rise of the network society, Castells (1996, p. 371) predicted increasing social stratification among users such that "the multimedia world will be populated by two essentially distinct populations: the *interacting* and the *interacted*, meaning those who are able to select their multidirectional circuits of communication, and those who are provided with a restricted number of prepackaged choices" or *acted upon*. The consequence of this disparity in technology use leads to what van Dijk (2000, 2005) identifies as a "usage gap" between different segments of the population, where well-placed users make far greater use of advanced applications at work, home, and school settings while *mis*placed users seek online amusement, game playing, and entertainment, and perhaps "infotainment" experiences. As computers continue to diffuse internationally, hardware penetration rates have risen but usage gaps have grown, with differences rising between simple and advanced information uses among different socioeconomic groups (van Dijk, 2005).

The issues involved in processing content and successfully navigating networked systems should be familiar to communication technology researchers and we should take opportunities like this to remind policy makers of the challenges confronting ordinary users. Not every audience member is equally equipped to contend with the demands of networked media and the array of complex message flows swirling about and enveloping society. This presents a challenge to message producers, who cannot assume uniform competencies across different strata of the social order, and to communication scholars, who must remain cognizant that most members of the media audience do not even possess a college degree. The great promise of mass communication—to uplift and edify the masses—will only ever be partially realized if media producers, scholars, and critics continue to operate under the incorrect assumption that all audience members are highly sophisticated, civically and informationally engaged, technically literate, and textually oriented; they are not—and so we must understand and meet the mass audience where its skills and motivations are rather than where we wish them to be.

References

Anderson, A. A., Brossard, D., Scheufele, D. A., Xenos, M. A., & Ladwig, P. (2013). The “nasty effect:” Online incivility and risk perceptions of emerging technologies. *Journal of Computer-Mediated Communication, 19*(3), 373–387.

Bennett, W. L., & Segerberg, A. (2013). *The logic of connective action: Digital media and the personalization of contentious politics*. New York: Cambridge University Press.

Bessiere, K., Ceaparu, I., Lazar, J., Robinson, J., & Schneiderman, B. (2004). Social and psychological influences on computer user frustration. In E. P. Bucy & J. E. Newhagen (Eds.), *Media access: Social and psychological dimensions of new technology use* (pp. 91–103). Mahwah, NJ: Lawrence Erlbaum Associates.

Beyer, Y., Enli, G. S., Maaso, A. J., Ytreberg, E. (2007). Small talk makes a big difference: Recent developments in interactive, SMS-based television. *Television and New Media, 8*(3), 213–234.

Bonnington, C. (2015, February 10). In less than two years, a smartphone could be your only computer, *Wired*. Retrieved from https://www.wired.com/2015/02/smartphone-only-computer/

Bolter, J. D., & Grusin, R. (2000). *Remediation: Understanding new media, rev. ed*. Cambridge, MA: MIT Press.

Bordewijk, J. & van Kaam, B. (1986). Towards a new classification of tele-information services. *Intermedia, 14*(1), 16–21.

Bucy, E. P. (2004). The interactivity paradox: Closer to the news but confused. In E. P. Bucy & J. E. Newhagen (Eds.), *Media access: Social and psychological dimensions of new technology use* (pp. 47–72). Mahwah, NJ: Lawrence Erlbaum Associates.

Bucy, E. P., & Newhagen, J. E. (2004). *Media access: Social and psychological dimensions of new technology use*. Mahwah, NJ: Lawrence Erlbaum Associates.

Bucy, E. P., & Zelenkauskaite, A. (2014, October). Big Data and unattainable scholarship. In S. P. Gangadharan, V. Eubanks, & S. Barocas (Eds.), *Data and discrimination: Collected essays*, pp. 21–25. Washington, DC: Open Technology Institute, New America Foundation. Retrieved from http://newamerica.org/downloads/OTI-Data-an-Discrimination-FINAL-small.pdf

Bush, V. (1945, July). As we may think. *The Atlantic*. Retrieved from http://www.theatlantic.com/magazine/archive/1945/07/as-we-may-think/3881/

Castells, M. (1996). *The rise of the network society*. Oxford: Blackwell.

Castells, M. (2007). Communication, power, and counter-power in the network society. *International Journal of Communication, 1*, 238–266. Retrieved from http://ijoc.org/index.php/ijoc/article/viewFile/46/35

Castells, M. (2009). *Communication power*. New York: Oxford University Press.

Dale, D. (2016, October 19). Confessions of a Trump fact-checker. *Politico*. Retrieved from http://www.politico.com/magazine/story/2016/10/one-month-253-trump-untruths-214369

December, J. (1997). *The World Wide Web unleashed, 4th ed*. Carmel, IN: Sams Publishing.

Dvorak, J. C. (2012, December 4). Should we consider the smartphone a computer? *PC* magazine. Retrieved from http://www.pcmag.com/article2/0,2817,2412850,00.asp

Evans, E. J. (2008). Character, audience agency, and transmedia drama. *Media, Culture, & Society, 30*(2), 197–213.

Fallows, J. (1996). *Breaking the news: How the media undermine American democracy*. New York: Pantheon.

Garfinkel, S. (2000). *Database nation: The death of privacy in the 21st century*. Sebastopol, CA: O'Reilly Media.

Gilbert, D. T., Krull, D. S., & Malone, P. S. (1990). Unbelieving the unbelievable: Some problems in the rejection of false information. *Journal of Personality and Social Psychology, 59*(4), 601–613.

Gleick, J. (2000). *Faster: The acceleration of just about everything*. New York: Vintage Books.

Grossman, L. K. (1995). *The electronic republic*. New York: Penguin Books.

Hargittai, E. (2010). Digital na(t)ives? Variation in internet skills and uses among members of the "net generation." *Sociological Inquiry, 80*(1), 92–113.

Hargittai, E., & Shafer, S. (2006). Differences in actual and perceived online skills: The role of gender. *Social Science Quarterly, 87*(2), 432–448.

Hertsgaard, M. (1989). *On bended knee: The press and the Reagan presidency*. New York: Schocken Books.

Hoffman, D. L., & Novak, T. P. (1996). Marketing in hypermedia computer-mediated environments: Conceptual foundations. *Journal of Marketing, 60*(3), 50–68.

Howard, P. N. (2005). *New media campaigns and the managed citizen*. New York: Cambridge University Press.

Jenkins, H. (2008). *Convergence culture: Where old and new media collide*. New York: NYU Press.

Kalyanaraman, S., & Wojdynski, B. W. (2015). Affording control: How customization, interactivity, and navigability affect psychological responses to technology. In S. S. Sundar (Ed.), *The handbook of the psychology of communication technology* (pp. 425–444). New York: Wiley-Blackwell.

Kelly, K., & Wolf, G. (1997, March 1). Push! Kiss your browser goodbye: The radical future of media beyond the Web. *Wired*. Retrieved from https://www.wired.com/1997/03/ff-push/

Lasswell, H. D. (1948). The structure and function of communication in society. In L. Bryson (Ed.), *The communication of ideas* (pp. 37–51). New York: Harper & Row.

Markoff, J. (2016, November 17). Automated pro-Trump bots overwhelmed pro-Clinton messages, researchers say. *The New York Times*. Retrieved from https://www.nytimes.com/2016/11/18/technology/automated-pro-trump-bots-overwhelmed-pro-clinton-messages-researchers-say.html

Matthews, N. L., & Weaver, A. J. (2013). Skill gap: Quantifying violent content in video game play between variably skilled users. *Mass Communication and Society, 16*, 829–846.

McChesney, R. W. (2015). *Rich media, poor democracy: Communication politics in dubious times* (rev. ed.). New York: The New Press.

Morris, M., & Ogan, C. (1996). The Internet as mass medium. *Journal of Communication, 46*(1), 39–50.

Mutz, D. C. (2015). *In-your-face politics: The consequences of uncivil media*. Princeton: Princeton University Press.

Newhagen, J. E., & Bucy, E. P. (2004). Routes to media access. In E. P. Bucy & J. E. Newhagen (Eds.), *Media access: Social and psychological dimensions of new technology use* (pp. 3–23). Mahwah, NJ: Lawrence Erlbaum Associates.

Newhagen, J. E., & Levy, M. R. (1998). The future of journalism in a distributed communication architecture. In D. L. Borden & K. Harvey (Eds.), *The electronic grapevine: Rumor, reputation, and reporting in the new online environment* (pp. 9–21). Mahwah, NJ: Lawrence Erlbaum Associates.

Nowak, K., Krcmar, M., & Farrar, K. (2008). The causes and consequences of presence: Considering the influence of violent video games on presence and aggression. *Presence: Teleoperators & Virtual Environments, 17*(3), 256–268.

Ophir, E., Nass, C., & Wagner, A. D. (2009). Cognitive control in media multitaskers. *PNAS, 106*(37), 15583–15587.

Papacharissi, Z. (2015). *Affective publics: Sentiment, technology, and politics*. New York: Oxford University Press.

Rheingold, H. (2002). *Smart mobs: The next social revolution*. New York: Basic Books.

Rheingold, H. (2014). *Net smart: How to thrive online*. Cambridge, MA: MIT Press.

Rojas, V., Straubhaar, J., Roychowdhury, D., & Okur, O. (2004). Communities, cultural capital, and the digital divide. In E. P. Bucy & J. E. Newhagen (Eds.), *Media access: Social and psychological dimensions of new technology use* (pp. 107–130). Mahwah, NJ: Lawrence Erlbaum Associates.

Rosen, J. (2001). *The unwanted gaze: The destruction of privacy in America*. New York: Vintage Books.

Shneiderman, B. (2000). Universal usability. *Communications of the ACM, 43*(5). 85–91.

Silverman, (2016, November 16). This analysis shows how viral fake election news stories outperformed real news on Facebook. *Buzzfeed*. Retrieved from

https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook

Stoll, C. (1995). *Silicon snake oil: Second thoughts on the information superhighway*. New York: Anchor Books.

Stromer-Galley, J. (2014). *Presidential campaigning in the Internet age*. New York: Oxford University Press.

Van Dijk, J. (2000). Widening information gaps and policies of prevention. In K. L. Hacker & J. van Dijk (Eds.), *Digital democracy: Issues of theory & practice* (pp. 166–183). London: Sage.

Van Dijk, J. (2005). *The deepening divide: Inequality in the information society*. Thousand Oaks, CA: Sage.

Van Dijk, J. (2012). *The network society, 3rd ed*. Thousand Oaks, CA: Sage.

Wertime, D. (2016, May 19). Meet the Chinese trolls pumping out 488 million fake social media posts: New research exposes a “massive secretive operation” to fill China’s internet with propaganda. *Foreign Policy*. Retrieved from http://foreignpolicy.com/2016/05/19/meet-the-chinese-internet-trolls-pumping-488-million-posts-harvard-stanford-ucsd-research/

Zelenkauskaite, A., & Bucy, E. P. (2016). A scholarly divide: Social media, Big Data, and unattainable scholarship. *First Monday, 21*(5). http://dx.doi.org/10.5210/fm.v21i5.6358

Endnotes

[1] Rheingold (2002) years earlier made similar, though less theoretically grounded, observations in favor of the "ad-hocratizing" potential of mobile technology to facilitate temporary clustering around information or action agendas of mutual interest. More recently, he has written about the importance of digital literacy, including strategies for enhancing networked attention, participation, critical consumption of information ("crap detection"), and what he labels network smarts (Rheingold, 2014).

[2] A problem compounded by Trump's own tendency to spout, both verbally and through Twitter, daily barrages of false claims, especially while campaigning (Dale, 2016).

[3] The year 1996 was a watershed in two respects. First, the landmark Telecommunications Act of 1996 deregulated the cable industry and opened the door for unprecedented consolidation in television and radio, paving the way for the formation of Fox News and conservative control of talk radio (McChesney, 2015). The presidential election of 1996 was also the first in which campaign activities and information sources began to migrate online, promoting a managed—and ultimately hyperpartisan—approach to citizenship (Howard, 2005; Stromer-Galley, 2014).

[4] Newhagen and Levy (1998, p. 17) anticipated this quandary when the shift to online news platforms began in earnest, observing that, "[I]t is difficult to imagine how this verification function might work in a distributed architecture and, in its absence, the burden of verification may thus shift back to the audience. Interactive information searches will call on users to employ a set of highly effortful cognitive skills they may not now possess."

[5] At the same time, many television shows, particularly in the prime-time drama, public affairs, talent competition, and game show genres, are incorporating feedback mechanisms that allow the viewing audience to engage more with the program hosts, show characters, contestants, or even other viewers either in real-time or asynchronously through activities on second screens,

fan pages, show websites, text-on-television, telephone call-ins, and so on, creating rich "transmedia" experiences (see Beyer , Enli, Masso, & Ytreberg, 2007; Evans, 2008).

[6] Mindful of this problem, interactive companies like Chicago-based Jellyvision (creators of the *You Don't Know Jack* trivia game) have developed "conversational interfaces" that talk users through "big life decisions, like selecting a health insurance plan, saving for retirement, managing finances, and navigating a career. Our recipe: behavioral science, cutting-edge tech, great writing, purposeful humor, original animation, and oregano." The system works by allowing visitors to "interact in real-time with a virtual host or advisor who talks directly to you and helps you understand complicated stuff and make smarter decisions" (see www.jellyvision.com).

Journal of Communication Technology | JoCTEC

Published by the Communication Technology Division of AEJMC

Communication Challenges in Cybersecurity

Dr. Marcia W. DiStaso

Associate Professor and Chair

Department of Public Relations

Virginia Tech University

Correspondence:

352-273-1220

mdistaso@ufl.edu

Original manuscript accepted for publication in

Journal of Communication Technology

Published by the Communication Technology Division of the Association for Education in Journalism and Mass Communication

Communication Challenges in Cybersecurity

Abstract

Cyberattacks are becoming a part of daily life, but navigating before, during, and after an attack is far from routine. With reputations on the line, cybersecurity is much more than an IT problem. Strategic communication across entire organizations is necessary to successfully navigate cybersecurity. This article outlines cybersecurity and cyberattacks from a communication perspective and provides five cybersecurity communication challenges. Suggestions for further research are also included.

In the last decade, cybersecurity has emerged as a top priority in both government and business. Most individuals are likely aware that cyberattacks are increasing in frequency and in intensity, as many organizations confirm they have suffered at least one cyber incident (Weldon, 2016).

While cyberattacks are not a new phenomenon, their frequency and sophistication certainly continues to increase. In 2009 President Obama declared that “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity” (The White House, 2009, para 10). Then, in 2014, Assistant Attorney General John Carlin (2014, para 7) highlighted the pervasiveness of cyber threats at the U.S. Chamber of Commerce Third Annual Cybersecurity Summit when he referenced a statement by FBI Director James Comey who said, “there are two kinds of big companies in America: those who have been hacked . . . and those who don’t know they’ve been hacked.”

Cyberattacks such as those perpetrated against Sony Pictures Entertainment in late 2014 (see Elkind, 2015), Target in 2013 (see Kassner, 2015), Anthem in 2015 (see Herman, 2016), and Yahoo in 2016 (see Thielman, 2016) are worst-case scenarios for many organizations. A 2015 survey indicated that 82% of organizations list cyberattacks as one of their top three concerns (Information Systems Audit and Control Association, 2016). It is important to mention that cyberattacks do not exclusively affect for-profit organizations. Nonprofits, governmental agencies, and individuals are also frequent targets. In fact, the largest attack in 2015 was at OPM—the US Federal Office of Personnel Management—where highly sensitive security clearance form data was stolen (see Adams, 2016).

Cybersecurity has undoubtedly become a critical business challenge, and given the heightened media attention, cyberattacks are likely to be an increasing concern for the public as well. Recent political attention and intensified discussions about cyberattacks have led to much stronger governmental involvement. The Department of Homeland Security has a robust focus on cyberspace. As such, cybercrimes like child pornography, child exploitation conspiracies, banking and financial fraud, and intellectual property violations fall under their purview (Department of Homeland Security, 2016). Homeland Security actually has a dual role with cyberattacks where they are involved in helping the victim or the target of the malicious activity and in identifying and stopping the perpetrators of the attacks.

Today, cybersecurity is not simply an IT concern. Instead, it is a strategic brand, product, and service necessity (KPMG, 2016). Planning and strategy are critical, plus it is important to acknowledge that not all attacks can be prevented or even defended against (Coghian, 2016). Given the likelihood of being the victim of a cyberattack, many organizations are reconsidering their strategies and most have teams in place to focus on cybersecurity led by a Chief Information Officer (CIO), a Chief Information Security Officer (CISO), or a Chief Technology Officer (CTO).

In a 2016 study with C-suite members, researchers found that reputation with customers was the greatest concern (Coghian, 2016). Brand reputation is a fragile asset and probably the most important component of success given that it drives everything from growth to revenue. Plus, once a reputation is damaged, it is extremely difficult to repair (DiStaso, 2015). Cyberattacks have a high likelihood of being damaging to a company's reputation because the victim is not simply the company itself but also customers. That is, customers become victims of cyberattacks, too, because typically the information stolen exposes customers to identity theft or even financial losses.

Reputation expert Leslie Gaines-Ross identified what she calls a "negative halo effect" (Coghian, 2016, p. 2). In other words, a cyberattack on a company has the potential to impact every aspect about that company in the eyes of the public as they "go beyond the incident to question its products and controls" (Coghian, 2016, p. 2). Unfortunately, the actual cyberattack is just the beginning. Much of the impact from an attack will continue to unfold over years to come. In fact, Mossberg, Fancher, Gelinne, and Calzada (2016) identified that a cyberattack results in hidden (e.g., the investigation, customer notification, litigation fees, cybersecurity improvements) and unhidden costs (loss of revenue, loss of trust, loss of intellectual property, increase in insurance), and it is the hidden costs that account for about 90 percent of the total business impact. Much of this impact is does not occur until at least two years after the attack.

Given the precarious nature of the cyber environment, company executives are in a difficult situation. Consumers have many options, so patience and loyalty are commodities that are easily lost if a company is perceived as unprepared or lax in its security. By keeping in mind what is at risk, the trust of their customers, companies can work to build goodwill before the next big attack and plan ahead for how to keep communications as a critical component of managing an attack. With this lofty goal for companies in mind, this article identifies what cybersecurity is,

why it is so important to organizations, types of common cyberattacks, and five cybersecurity communications challenges. Suggestions for further research are also included.

Cybersecurity Defined

The word security is defined as "The state of being free from danger or threat" (Oxford Living Dictionary, n.d.). Then, considering that cyber refers to the computer, cybersecurity is likely to be considered as computers being free from danger or threat. However, the dictionary definition is, "The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this" (Oxford Living Dictionary, n.d.). This very broad definition really leaves open any actions of protection and is only concerned with the use of electronic data. The CyberSecurity Forum is a bit more specific in their definition: "the collection of technologies, processes, and practices that protect networked computer systems from unauthorized use or harm" (n.d., para 1). This definition still allows for any actions of protection but moves beyond just use to include harm. The ISO (the International Organization for Standardization) gets even more specific with their definition: "Preservation of confidentiality, integrity and availability of information in the Cyberspace" (International Organization for Standardization & International Electrotechnical Commission, 2012, p. 4.2). While each of these terms are helpful at understanding what cybersecurity may be, they still lack insight into where the threat comes from and if it is cyber that needs the protection or is doing the protecting (A deeper look into the definition can be found in Bay, 2016).

Certain industries are at a higher risk of being the target of a cyberattack. For example, companies in healthcare and financial services are much more likely to be attacked than those in other industries. The Internet of Things (IoT) also comes with increased concerns due to its interconnectedness and few endpoint protections. These "smart" objects such as thermostats,

baby monitors, and refrigerators provide added entries to networks and complicate cybersecurity efforts (Stavridis & Weinstein, 2016).

Ultimately, cybersecurity in public relations terms is about managing risk. This risk management includes digital technologies and efforts to maintain trust (van Kessel & Allan, 2015). Therefore, cybersecurity is much more than a technology issue, and it involves more than the IT department. It affects every level of an organization and every department and member of the C-Suite in different ways (van Kessel & Allan, 2015). IBM also talks about cybersecurity awareness being "knowledge combined with attitudes and behaviors that serve to protect our information assets. Being "cybersecurity aware" means you understand what the threats are and you take the right steps to prevent them" (Martin, 2014, para 4).

Why Cybersecurity Matters

Cybersecurity is challenging for every country (Tisdale, 2015) and every type of organization. Everyone is at risk including government agencies, the military, corporations, financial institutions, hospitals, retailers, nonprofits, universities, and all other groups that collect or store confidential information.

Cybersecurity is a costly business. A 2016 Ponemon Institute and IBM study found that the average cost of data breach was $4 million and the average cost per lost or stolen record containing sensitive and confidential information was $158. In early 2016, Juniper Research predicted that cybercrime will cost businesses over $2 trillion by 2019, noting that this amount accounts for four times the total in 2015 (2015). They indicated that the likely reasons for the increase would be in improved professionalism of hacktivism and bigger targets being attacked.

In 2014 a survey by Semafone, a fraud-protection company, found that 86% of respondents would not likely do business with a company that had a data breach of their credit card information (Williams & Levy, 2014). Then, in 2016 a survey by FireFly, a security vendor,

found 72% of consumers interviewed indicated they would probably stop buying from a company that had a breach because of improper cybersecurity (Muncaster, 2016).

Underprepared companies put customers, employees and all stakeholders at risk, so it is not surprising to see that companies found to have taken this risk and lost have paid high prices. For example, after the Target breach that leaked information for over 110 million customers, they saw a dip in sales and profits sank about 50% the following quarter. The share price fell and the CEO was fired (Kassner, 2015).

Time to identify and contain cyberattacks is of utmost concern. The 2016 Ponemon Institute and IBM found that it took the companies in their study an average of 201 days to identify a breach and 70 days to contain it. The best course of action is for organizations to disclose the full extent of the breach to customers and regulators as quickly as possible within the first 24 hours of discovery (Coghian, 2016). While complete details of the attack may not be fully known so soon, it is imperative to get out front of the news cycle and work to avoid a “slow drip of bad news” because this slow drip will likely frustrate stakeholders, prolong the news cycle and increase mistrust (Coghian, 2016, p. 4).

Newsworthiness of data breaches is often determined in part by the number of data records, or terabytes, stolen (Farrell, 2016). Identifying this amount is especially tricky for organizations because number reporting needs accuracy and often definite totals are simply not available. Having to increase the number originally reported will likely trigger another news cycle and concerns about control of the attack. However, reporting a number too high may falsely escalate concern and negative media coverage.

Many companies that experienced a cyberattack also find themselves the target of shareholder and/or customer lawsuits. While 52% of people interviewed in a UK study of consumers said they would seek legal action of their information had been compromised by a company (Muncaster, 2016), what happens in the courts is quite interesting. Clearly, one can

make a case that a data breach creates a risk of future injury from identity theft or fraud and this risk is likely to cause some individuals anxiety. However, harm is needed to identify if a claim is viable. Alleged harm or potential harm is the aspect that has courts reaching inconsistent rulings (Solove & Citron, 2016).

Farrell (2016) indicated that companies should not "underestimate the power of an apology" (p. 3). It is likely that this recommendation comes from the 2014 Ponemon Institute report that found 43% of their respondents would be prevented from "discontinuing a relationship" with a company that had a data breach if they issued "[a] sincere and personal apology" (2016, p. 8).

Types of Cyberattacks

There are many different types of cyberattacks and new types are likely to continue to crop up. Each attack can have a different combination of the four elements of a cyberattack: Actor, Target, Effect, and Practice. Each element along with some of the more common options for that element are explained below.

Actors:

This element looks at who will conduct the attack. Common actors include cyber terrorists (often the goal is an attack designed to cause alarm or panic), nation-sponsored groups (who attack on behalf of geo-political objectives), hacktivist (an individual who wants to get attention for a cause), organized crime (groups who intend to engage in illegal activity), individuals (a person acting on their own), etc.

Targets:

This element looks at what was attacked. Common targets include social media accounts, email accounts, customer accounts, cloud accounts, point of sale systems, websites, financial networks, cellular networks, credit cards, etc.

Effects:

This element looks at the result of the attack. Common effects include data stolen/leaked, personal information stolen, account hijacked, damaged reputation, financial loss, data destroyed, vandalism, fraud, loss of trust, etc.

Methods:

This element looks at what was used to carry out the attack. Common methods of cyberattacks include:

- Data Breach – A data breach occurs when "sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so" (Rouse, 2016). Oftentimes, this attack targets financial or medical information but could also include trade secrets or intellectual property (Trend Micro, n.d.).
- Phishing Attacks – Phishing is probably the most common cyberattack. With this method hundreds of emails are sent with the hope that someone will open the attachment in the email or click a link with both actions giving them access to that computer or network (Lord, 2016).
- Social Engineering or Whaling – This type of attack is targeted and often is conducted by using what looks like an email from a top company executive requesting that a money wire be processed. This method is an elaborately engineered scheme that has cost companies billions of dollars because people did not realize the request was not actually from their CEO (Boulton, 2016).
- Malware – Malware is a term that applies to code that is installed on the computer such as Trojans, viruses, adware, and worms (Massachusetts Institute of Technology, 2016). This code is used to steal data or destroy something on the computer.

- Ransomware – Ransomware is an attack on a computer, system, or data that renders it unusable until a ransom is paid. Each situation is different but sometimes the only way to get the files or data back is to pay if backup is not available. A trend Micro study found that 77% of the US organizations they surveyed had never paid an attack ransom but 54% acknowledged that doing so is the easiest way to restore business (Field, 2016).

Communication Challenges

No matter the cause of the cyberattack, having to contact stakeholders (i.e., employees, stockholders, and customers) to tell them your organization has lost their data is not only a difficult exercise but also one that holds a potentially significant reputational risk. This reputation risk is especially true considering how quickly and easily information is shared on social media. When considering cybersecurity, organizations need to keep the communications elements in mind before, during, and after a cyberattack.

Communication Challenge #1: Cybersecurity requires a culture of risk.

Benjamin Franklin is often credited as saying, “By failing to prepare, you are preparing to fail” (see Mayberry, 2016). Operating in a culture of risk means that the company’s default expectation should be that it is at risk of losing its reputation. Additionally, organizations should conduct a risk assessment to identify the level of risk, in relation to cyberattacks, that they are willing to tolerate. Not all organizations are the same, so levels of tolerance are different and subsequently so are levels of cybersecurity.

With trust and loyalty of stakeholders on the line, risk assessment and crisis plans need to address stakeholder engagement in the event of a data breach. Additionally, given the frequent changes in technology, crisis plans should be updated regularly. Mock tests or simulations of plans are an excellent way to work toward being prepared. All plans should be fully aligned with IT’s operational cybersecurity plan and the business continuity plan. The role

of communications should be included in all plans so expectations are clear and will not need to be developed or negotiated in the middle of a cyberattack crisis.

Communication Challenge #2: Cybersecurity should not be "owned" by any department.

By having a seat at the executive table, members from IT, legal, production, communications, compliance, and all other departments can work together to identify possible warning signals. In isolation a singular odd situation may seem just odd, but when considered with other odd situations the oddity may indicate a reason for concern. As such, frequent cross-department meetings with company boards and senior management teams can serve as an excellent early warning system. Additionally, having multiple departments and individuals working together can help provide a more consistent application of policies.

Communication Challenge #3: The public shares some level of cybersecurity responsibility.

Many security experts believe that the weakest link in cybersecurity is humans. In fact, some data breaches are the result of human error. Aside from the errors made (intentionally or unintentionally) in or on behalf of a company, many cyberattacks are the result of individuals making a mistake. While it is highly likely that many people understand that there are risks with being online, it is possible that many do not know what their role is. Unless someone has personally been impacted or knows someone close that has, for example, had their identity stolen, he or she is unlikely to really understand. As such, cyber-safety can be considered a topic that is subject to education gap. If individuals better understood how their actions in social media and online place them at risk, some of the cyberattacks may be easier to prevent.

Communication Challenge #4: Cyberattacks are ever-changing.

Practicing effective cybersecurity is like aiming at a moving target. As technology improves so do cyberattacks. Plus, the volume of attacks can make their prevention especially challenging because companies rarely get a break between attacks and can even be the victim

of more than one at a time. The future of cybersecurity involves a high amount of uncertainty. Most likely, the unknown threats of today are the ones that will trouble companies tomorrow.

Meeting regulatory compliance mandates is also challenging since they can also frequently change. Speed is critical during a cyberattack, but legal and operational considerations are imperative to ensure proper handling of the crisis. Before a cyberattack, teams should be familiar with the relevant state and federal reporting and disclosure requirements for a breach.

Communications Challenge #5: Situational Perspective is Essential.

Often organizations do not know they have been breached for days, weeks, or even months. Once discovered, how the breach is handled is a critical element in the impact on reputation. Most stakeholders will not be worried about how the attack happened, so the best course of action is for the management team to communicate about how they will fix it. News spreads fast, so responding must be quick as well. This early communication will heavily influence both responses and reactions from the media and stakeholders. Messaging should focus on the stakeholder receiving the information in the form of straightforward and transparent facts.

Future Research Recommendations

Cybersecurity and cyberattack research is still relatively scarce, and few studies exist beyond the IT or technology realm. While further research is definitely needed into metrics, models, discovery, and analysis into security management, counterintelligence and vulnerabilities, additional research from a communications perspective is also needed. Specifically, research is needed in the following areas:

Collaboration – Information sharing is essential to protecting organizations, the government, and individuals. Furthermore, having countries work together would greatly

increase the information resources. Through collaboration, cybersecurity efforts can be furthered. While the Department of Homeland Security has developed and implemented numerous information sharing programs, the fruitfulness of these programs are to be determined. Research should be conducted to monitor and improve collaboration efforts.

Cyber education – There were 1 million cybersecurity job openings in January 2017 (Morgan, 2017). The reason for such a high number of jobs is the lack of education and training available. Given this deficit, research can be conducted to identify what role companies need and what specific skills are missing from traditional IT graduates.

Media's influence – The media plays a fundamental role with cyberattacks just as they would with any other crisis, but somehow some cyberattacks manage to receive little or no media coverage. Given the continuous cycle of cyberattacks in the news, research can be conducted to identify trends in the coverage and connect that with actions from the organization.

Stakeholder impact – A loss of trust and an impact on stakeholder relationships can be difficult to overcome. Research is needed to explore stakeholder expectations when it comes to cybersecurity and cyberattacks.

Planning ahead – Current efforts and research on cybersecurity are on "catch-and-patch" leaving little insight beyond current strategy. Therefore, proactive research is needed to explore what cyber challenges can be expected on the horizon along with insight into technological and communications means of managing the attack.

Case studies – Case studies that outline cyberattacks are extremely helpful to organizations and can provide excellent learning opportunities for students and scholars. Of special interest would be cases where there are impediments to communications as a result of the attack.

Conclusion

The purpose of this article was to highlight cybersecurity as a communications challenge, not just an IT one. Unfortunately, many organizations prioritize cybersecurity from an IT angle exclusively (Coghian, 2016). Yet, many CEOs have indicated that the greatest damage cyberattacks can cause is in loss of reputation. With the brand in mind, organizations need a "unity of purpose" (Coghian, 2016, p. 3), and without it executives can find this state of incongruence causes dissonance and subsequently ineffective action.

Many reports on cybersecurity and data breaches were reviewed for this article, and in this process what became glaringly obvious is the minimal mention of communication in most of them. Additionally, few mentioned anyone in the C-suite aside from the CIO – Chief Information Officer. By only focusing on cybersecurity as an IT problem, organizations are being extremely shortsighted and communications research can help explore the messaging around cyberattacks and how companies can control the damage, thereby filling the deep cybersecurity research gap.

References

Adams, M. (2016, March 11). Why the OPM hack is far worse than you imagine. *Lawfare*. Retrieved from https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine

Bay, M. (2016). What is cybersecurity? *French Journal for Media Research. Retrieved from* http://frenchjournalformediaresearch.com/index.php?id=988

Boulton, C. (2016, April 21). Whaling emerges as major cybersecurity threat. *CIO*. Retrieved from http://www.cio.com/article/3059621/security/whaling-emerges-as-major-cybersecurity-threat.html

Carlin J. (2014, October 28). Remarks by Assistant Attorney General John Carlin. U.S. Chamber of Commerce Third Annual Cybersecurity Summit. Washington, DC United

States. Retrieved from https://www.justice.gov/opa/speech/remarks-assistant-attorney-general-john-carlin-us-chamber-commerce-third-annual

Coghian, W. (2016). Protecting the brand—cyber-attacks and the reputation of the enterprise. *The Economist*. Retrieved from https://www.eiuperspectives.economist.com/technology-innovation/cyber-chasm-how-disconnect-between-c-suite-and-security-endangers-enterprise-0/article/protecting-brand—cyber-attacks-and-reputation-enterprise

CyberSecurity Forum (n.d.). Cybersecurity overview – all you need to know. Retrieved from http://cybersecurityforum.com/cybersecurity-overview/

Department of Homeland Security. (2016, September 27). *Cybersecurity*. Retrieved from https://www.dhs.gov/cybersecurity-overview

Department of Homeland Security. (2011). *Enabling distributed security in cyberspace: Building a healthy and resilient cyber ecosystem with automated collective action*. Retrieved from https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf

DiStaso, M. W. (2015). How Occupy Wall Street influenced the reputation of banks with the media. *Corporate Reputation Review*, *18*(2), 99–110.

Elkind, P. (2015, June 25). Sony Pictures: Inside the hack of the century. *Fortune*. Retrieved from http://fortune.com/sony-hack/

Farrell, S. (2016, July 22). Big hack attack: Protecting corporate reputation and brand value in the wake of a data breach. *The Public Relations Strategist*. Retrieved from http://www.prsa.org/Intelligence/TheStrategist/Articles/view/11571/1129/Big_Hack_Attack_Protecting_Corporate_Reputation_an#.WHuGS4WcGJM

Field, T. (Ed.). (2016). *Ransomware response study*. Retrieved from http://f6ce14d4647f05e937f4-4d6abce208e5e17c2085b466b98c2083.r3.cf1.rackcdn.com/2016-ransomware-response-study-pdf-3-w-2983.pdf

Herman, B. (2016, March 30). Details of Anthem's massive cyberattack remain in the dark a year later. *Modern Healthcare*. Retrieved from http://www.modernhealthcare.com/article/20160330/NEWS/160339997

Information Systems Audit and Control Association. (2016). *State of cybersecurity: Implications for 2016*. Retrieved from http://www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf

International Organization for Standardization & International Electrotechnical Commission, Joint Technical Committee ISO/IEC JTC 1. (2012). Information technology – Security techniques – Guidelines for cybersecurity. ISO/IEC 27032:2012(en). Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

Kassner, M. (2015, Feb. 2). Anatomy of the Target data breach: Missed opportunities and lessons learned. *ZDNet.* Retrieved from http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

KPMG (2016). *Consumer loss barometer*. Retrieved from https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2016/08/consumer-loss-barometer-v1.pdf

Lord, N. (2016, October 12). What is a phishing attack? Defining and identifying different types of phishing attacks. *Digital Guardian*. Retrieved from https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-different-types-phishing-attacks

Martin, J. (2014, October 1). Cybersecurity awareness is about both ‘knowing’ and ‘doing.’ *SecurityIntelligence*, Retrieved from https://securityintelligence.com/cybersecurity-awareness-is-about-both-knowing-and-doing/

Massachusetts Institute of Technology. (2016). Viruses, spyware, and Malware. *Information Systems and Technology*. Retrieved from https://ist.mit.edu/security/malware

Mayberry, M. (2016, April 22). By failing to prepare, you are indeed preparing to fail. *Entrepreneur*. Retrieved from https://www.entrepreneur.com/article/274494

Morgan, S. (2017, January 6). 1 million cybersecurity job openings in 2017. *CSO*. Retrieved from http://www.csoonline.com/article/3155324/it-careers/1-million-cybersecurity-job-openings-in-2017.html?upd=1484340060345

Mossburg, E., Fancher, D., Gelinne, J., & Calzada, H. (2016). Beneath the surface of a cyberattack. Retrieved from https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

Muncaster, P. (2016, May 13). Brits shun brands following breaches. *InfoSecurity*. Retrieved from https://www.infosecurity-magazine.com/news/brits-shun-brands-following/

Oxford Living Dictionary (n.d.). Retrieved from https://en.oxforddictionaries.com/

Ponemon Institute & IBM. (2016). *2016 cost of data breach study: Global analysis*. Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN

Rouse, M. (2016). Data breach. *TechTarget.* Retrieved from http://searchsecurity.techtarget.com/definition/data-breach

Solove, D. J., & Citron, D. K. (in press). Risk and anxiety: A theory of data breach harms. *Texas Law Review, 96*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638

Thielman, S. (2016, December 15). Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached

Smith, S. (2015, May 12). *Cybercrime will cost businesses over $2 trillion by 2019*. Retrieved from https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

Stavridis, J., & Weinstein, D. (2016, November 3). The Internet of Things is a cyberwar nightmare. *Foreign Policy (FP)*. Retrieved from http://foreignpolicy.com/2016/11/03/the-internet-of-things-is-a-cyber-war-nightmare/

Tisdale, S. M. (2015). Cybersecurity: challenges from a systems, complexity, knowledge management and business intelligence perspective. *Issues in Information Systems, 16*(3), 191–198.

Trend Micro (n.d.). *Data breach*. Retrieved from http://www.trendmicro.com/vinfo/us/security/definition/data-breach

van Kessel, P., & Allan, K. (2015). *Creating trust in the digital world*. Retrieved from http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

Weldon, D. (2016, August 24). A deeper look at business impact of a cyberattack. *CIO*, Retrieved from https://www.cio.com/article/3112617/data-breach/a-deeper-look-at-business-impact-of-a-cyberattack.html

The White House, Office of the Press Secretary. (2009). *Remarks by the President on Securing our Nation's Cyber Infrastructure*. Retrieved from https://obamawhitehouse.archives.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

Williams, X. V., & Levy, F. (2014, March). Eighty-six percent of customers would shun brands following a data breach. Retrieved from https://semafone.com/press-releases-us/86-customers-shun-brands-following-data-breach/?lang=us