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