Information Security in an Age of Sharing

Thomas Corcoran

DeVry University

February 4, 2018

Information Security in an Age of Sharing

With the advent and widespread use of social media, sharing has become the norm for most people. Using technologies such as Twitter, Facebook and Instagram, to name a few, people share more details of their day-to-day lives than ever before. These technologies exist for sharing and encourage users to share as much information as they would like. As of January 2018, there are over 2 billion monthly active Facebook users during the third quarter of 2017. Daily, the "Like" and "Share" buttons are viewed on close to 10 million websites (Noyes, 2018). Twitter boasts similar sharing statistics with nearly 6,000 tweets being posted every second as of 2016 (Sayce, Unknown Date). The total number of tweets sent per day is roughly 500 million (Aslam, 2018). This environment of sharing directly contrasts with business needs for information security. It seems like each month we hear about a new case of retail hacking or identity theft (Telegraph.co.uk, 2017). This can result in a loss of consumer confidence in a retail businesses and payouts of millions of dollars as a result of these data breaches (Riley & Pagliery, 2015). So, to say information security is important is an understatement. Corporations, governments, financial institutions, hospitals and colleges, to name a few, all obtain and store massive amounts of data about consumers, patrons, patients and students. This data might be in the form of bank account numbers, credit card numbers, social security numbers, user ids/passwords, and other confidential and personally identifiable information, let alone any budget, stock, or research and development information which could give a corporation a competitive advantage. All of this highlights the need for information security. This paper will discuss some of the options businesses have for keeping information secure and specifically securing Adobe PDFs for clients when designing infographics.

Some estimates have determined that 2.5 Quintillion bytes of data is created each day (Jacobson, 2013). Since businesses rely so heavily on data driven decisions, that data should be treated as one of the most valuable commodities of the businesses. Part of the solution to treating information as a valued commodity would be to keep it safe while still granting access to the correct employees, just like people put money into a bank account rather than just letting this valuable asset be unprotected by keeping it around the house. Analogously, the money is safe and yet still available to withdraw from the bank by the correct account holder. Several options exist for securing information contained in electronic and/or print documents including, 1) Encryption/Password Protection, 2) Email Tracking, 3) Shredding Documents, and 4) Limiting Physical Building Access (Krum, 2013). Options 1 and 2 are methods for securing electronic files whereas options 3 and 4 would be primarily for securing physical paper documents. First, file encryption allows a document or folder containing documents to be locked so only persons with the correct decryption key or password can open those electronic assets. Several commercial products are available for both Mac and Windows PC platforms for encrypting folders/files (Rubenking, 2017). This keeps the files safe in as far as only the correct persons have access to the decryption key. Specifically, Adobe PDFs with confidential business information can be secured using password protection to restrict the opening, printing, or editing of those documents. Secondly, email tracking allows a business to see exactly who opened an email by IP address, when an email was opened, and if attachments and links were clicked within the email. Using email trackers, all of this data is supplied back to the email sender automatically (Gotter, 2017). In addition to these two electronic file safeguarding methods, physical documents also require securing. By creating and enforcing a corporate policy on shredding documents, corporations can secure physical copies of sensitive information by destroying older copies.

Sadly, many businesses believe that physical document might be safer than electronic information with all of the data breaches frequenting the news, but according to research, in companies of fewer than 500 employees, 61% of data breaches happened with paper documents (McGee, 2014). Lastly, limiting physical access to buildings can help secure confidential documents by only allowing the internal employees and granting external vendors, partners, and guests access to the businesses premises. Personally, I have never worked at such a business, but I have interviewed for a job at a large insurance agency which required all employees to use a keycard to grant access to the buildings, as well as visitors, like myself in that case, to have made arrangements to be escorted throughout the premises after checking in and being vetted by security personnel. These four options are just the start of a larger information security policy corporations should adopt to keep their information secure and yet still accessible by the correct employees.

One the one hand, our society shares more information through social media than was possible prior to social media technologies. However, businesses still have a responsibility to keep confidential and personally identifiable information secure and private. Following the appropriate level of protection(s) should go a long way toward safeguarding this sensitive information. As shown in this paper, when it comes to confidential and personally identifiable information there is a need for securing information and plenty of options available.

References

Aslam, S. (2018, January 1). Twitter by the numbers: Star, demographics & fun facts. [Blog post]. Retrieved from https://www.omnicoreagency.com/twitter-statistics/

Gotter, A. (2017, May 2). The 5 (+5) best email tracking services of 2017. [Blog post]. Retrieved from https://adespresso.com/blog/5-best-email-tracking-services-know-when-your-email-has-been-opened/

Jacobson, R. (2013, April 24). 2.5 quintillion bytes of data created every day. How does CPG & Retail manage it? [Blog post]. Retrieved from https://www.ibm.com/blogs/insights-on-business/consumer-products/2-5-quintillion-bytes-of-data-created-every-day-how-does-cpg-retail-manage-it/

Krum, R. (2013). Cool Infographics: Effective Communication with Data Visualization. Indianapolis, IN: John Wiley & Sons.

McGee, M. (2014, June 16). Preventing breaches: Dont' forget paper. [Blog post]. Retrieved from http://www.databreachtoday.com/blogs/preventing-breaches-dont-forget-paper-p-1690

Noyes, D. (2018, January 4). The top 20 valuable Facebook statistics - updated January 2018. [Blog post]. Retrieved from https://zephoria.com/top-15-valuable-facebook-statistics/

Riley, C. & Pagliery J. (2015, March 19). Target will pay hack victims $10 million. [Blog post]. Retrieved from http://money.cnn.com/2015/03/19/technology/security/target-data-hack-settlement/index.html

Rubenking, N. (2017, December 12). The best encryption software of 2018. [Blog post]. Retrieved from https://www.pcmag.com/article/347066/the-best-encryption-software-of-2016

Sayce, D. (Unknown data). Number of tweets per day? [Blog post]. Retrieved from https://www.dsayce.com/social-media/tweets-day/

Telegraph.co.uk. (2017, August 14). Cyber attacks on online retailers double in a year as hackers try to steal shoppers' details. [Blog post]. Retrieved from http://www.telegraph.co.uk/news/2017/08/13/cyber-attacks-online-retailers-double-year-hackers-try-steal/