ASA

Annie Searle & Associates LLC

**Research Note**

# Ashley Madison and Managing a Risky Business

Kevin Rawls

January 2016



Keywords: Privacy, Data Security, Ashley Madison, Data Breaches, Risk Management.

*Abstract: Cheating is risky business – when your business model is built upon cheating, it adds an entirely new level of risk. The website AshleyMadison is a now notorious website built around enabling married people to have extramarital affairs, that in 2015 experienced a very severe data breach of its customers' data. This paper explores some of the heightened levels of internal and external risks faced by a business that operates in a legally sound but morally compromised space.*

## Introduction

Ashley Madison considers itself the world's leading married dating service for "discreet encounters." What that means in plain English is that it is a website to help married people cheat on their spouses. While not illegal, Ashley Madison has gotten a lot of recent attention for providing such a morally dubious service. Attention that is understandably negative and from many people who feel compelled to fight back against a company whose slogan is "Life is short, have an affair."[i] In an enterprise rooted in such a morally questionable foundation and with millions of users, lots of media attention, and vast amounts of highly sensitive data, risk management is extremely important for their success. However, with this high risk comes many potential control failures, the most threatening of which include internal events and external events.

## Internal Events

Internal events at Ashley Madison could and have proven to be extremely dangerous to their enterprise. For example, in 2012 the company was sued by former employee Doriana Silva. She claimed that she had suffered a wrist injury from being overworked on a project involving

[i] www.ashleymadison.com

creating thousands of female bots for their website.[1] Why was she creating so many bots? The stark truth of their website is that only approximately 12,000 of their 5.5 million users are female, less than 1 percent.[2] At the same time, Ashley Madison offers their customers a "guarantee"[3] that users will find a match by using their service. To compensate for this very high discrepancy the company has reportedly made over 70,000 bots, some 3,000 of which were tasked to Silva over a three week period in preparation for their new Portuguese website. In 2015, the Ontario Superior Court dismissed the case leaving the company reportedly "very pleased."[4] Ashley Madison also alleged that Silva had kept confidential documents and sought to retrieve them.

It is clear from these reports that their internal workings are sometimes harsh and shady, which is understandable given the nature of their business. However, this creates a very large potential for control failure by unhappy and disgruntled employees. It is enough that their work is considered morally wrong by most societies, and that they are often the recipients of criticism and judgment. Ashley Madison as a company then adds on to this, working their employees to the point of lawsuit, whether the lawsuits are successful or not. This undoubtedly fosters an internal culture of unhappy employees, employees who have access to highly sensitive data that could potentially tarnish the already negative reputation of their company. This ticking time bomb of an internal working environment is undoubtedly a risk management nightmare that could easily start a domino effect ending in disaster. A potential control failure in this aspect of the company is a crucial thing to consider when evaluating risk for Ashley Madison.

In terms of managing internal risk, they could do many things differently. They could start by giving their employees better working conditions and not working them to the point of injury. In a business where the employees are doing work that could potentially risk the reputation and safety of a company, it would be a prudent to treat them well - particularly when they have access to highly sensitive documents that could damage the company if leaked. A more delicate approach to administration might do wonders for managing the risk of internal events at Ashley Madison.

**External Events**

While internal events are a massive risk management concern, it is clear that their largest potential for control failure lies in external events. The uncontested best example of this is the massive data breach that occurred in July of 2015, where over 60 gigabytes of data containing user details were leaked. This attack was orchestrated by a group calling themselves "The Impact Team" on July 15th 2015.[5] After the breach, The Impact Team threatened Ashley Madison's parent company Avid Life Media (ALM), saying they would release user data if they did not shut down AshleyMadison.com and its sister site EstablishedMen.com. ALM did not back down and on August 18th a 10 gigabyte compressed archive confirmed by experts was leaked to the Internet with user profile information from AshleyMadison.com. ALM promptly responded by calling out The Impact Team, saying, "This event is not an act of hacktivism, it is an act of criminality. It is an illegal action against the individual members of AshleyMadison.com, as well as any freethinking people who choose to engage in fully lawful online activities."[6] Two days later, a second and even larger data dump was leaked (12.7GB) including the email of ALM CEO Noel

Biderman. A week later Biderman stepped down from his position as CEO.[7]

The Ashley Madison data breach was a massive blow to the reputation of an already unpopular company but the final nail in the coffin came in the form of a failed promise uncovered in the data. The attack was allegedly fueled by the company's guarantee that if customers wanted to, they could pay a $19 dollar fee and have all of their information permanently deleted from their site, an option that earned the company more than $1.7 million dollars.[8] This was determined to be a lie when the hackers leaked data from accounts that had paid to have the data deleted. This caused massive outrage among customers and ended in a $576 million dollar class action lawsuit against the company.[9]

**Risk Management**

The data breach highlights how catastrophic a control failure in the security from outside events can be for a company like Ashley Madison. Data security should be the highest priority for an enterprise with a business model so widely considered to be morally wrong, and as Match.com co-founder Trish McDermott puts it, "a business built on the back of broken hearts, ruined marriages, and damaged families."[10] The highly sensitive environment of their company was clearly not taken into enough consideration and after what can only be described as a complete and utter failure in control, they were left with a tarnished reputation and millions of dollars in loss.

There are numerous things Ashley Madison could have done to prevent - or at least lessen the blow of - the data breach. They could have taken the time to consider just how sensitive their data is, not just for the reputation of their company but also for the personal lives of their customers. More resources, money, and time could have been invested in the security of their data rather than other expenses, such as an attempted super bowl ad in 2009.[11]

Another example and one of the biggest things Ashley Madison failed to do which could have greatly alleviated the situation was encrypt their data. The data that they promised would be deleted through their "full delete" option not only not deleted, it was not encrypted at all. This meant the hackers had to go through very little effort to expose all the secrets in those files. A general higher sense of attention and care might have gone a very long way in controlling their risks.

**Conclusion**

Ashley Madison is a company that provides a very risky service, but ironically has failed in controlling their own risks. Some might consider it poetic that a website intended to help people cheat on their spouses was taken down in the way that they were. Nevertheless, the site was not completely taken down, and today anyone can still go on AshleyMadison.com and make an account. The data breach showed them and the world how necessary managing risky business can be. The only way Ashley Madison can bounce back from this catastrophe is to put much more time, money, and effort into risk management.

[1] "Woman Hurt Typing Fake Profiles for Dating Site, $20M Suit Alleges." *CityNews*. 10 Nov. 2013. Accessed Dec. 2015 <www.citynews.ca>.

[2] Reed, Brad. "The Most Hilarious Revelation about the Ashley Madison Hack Yet." *Yahoo Tech*. 27 Aug. 2015. Accessed Dec. 2015 <www.yahoo.com/tech>.

[3] "The Ashley Madison Affair Guarantee Program." Ashley Madison. N.D. Accessed Dec. 2015 <www.ashleymadison.com>.

[4] Loriggio, Paola. "Lawsuit Against Dating Site for Married People Seeking Affairs Dismissed." *The Globe and Mail*. 18 Jan. 2015. Accessed Dec. 2015 <www.theglobeandmail.com>.

[5] "Online Cheating Site AshleyMadison Hacked." *Krebs On Security*. 15 Jul. 2015. Accessed Dec. 2015 <www.krebsonsecurity.com>.

[6] Zetter, Kim. "Hackers Finally Post Stolen Ashley Madison Data." *Wired*. 18 Aug. 2015. Accessed Dec. 2015 <www.wired.com>.

[7] Perlroth, Nicole. "Ashley Madison Chief Steps Down After Data Breach." *The New York Times*. 28 Aug. 2015. Accessed Dec. 2015 <www.nytimes.com>.

[8] Welch, Chris. "Ashley Madison's $19 'Full Delete' Option made the Company Millions." *The Verge*. 19 Aug. 2015. Accessed Dec. 2015 <www.theverge.com>.

[9] Loriggio, Paola.

[10] Farrell, Paul. "Ashley Madison Hacked: 5 Fast Facts You Need to Know." *Heavy*. 20 Jul. 2015. Accessed Dec. 2015 <www.heavy.com>.

[11] Hill, Catey. "Banned! These Ads Are Too Racy for the Super Bowl." *Daily News*. 29 Jan. 2009. Accessed Dec. 2015 <www.nydailynews.com>.