IBS Center for Management Research

Ashley Madison Hacking: The Dark Web Gets Even Darker

This case was written by ***Koti Vinodbabu,*** *under the direction of* ***Debapratim Purkayastha,*** *IBS Hyderabad. It was compiled from published sources, and is intended to be used as a basis for class discussion rather than to illustrate either effective or ineffective handling of a management situation.*

IBS Center for Management Research (ICMR)
IFHE Campus, Donthanapally,
Sankarapally Road, Hyderabad-501 203,
Telangana, INDIA.
Ph: +91 9640901313
E-mail: casehelpdesk@ibsindia.org

ICMR
IBS Center for Management Research
www.icmrindia.org

Ashley Madison Hacking: The Dark Web Gets Even Darker

"The day will come when we look back at the major cyber security incidents of 2015. There is little doubt that the Ashley Madison incident will be the most fascinating in many minds for some time to come."[1]

– John McAfee, a commentator on Cybersecurity, in 2015.

"We're seeing a lot of hacktivism coming from the political and the geopolitical perspective as well as the social justice perspective. We're living in a really dangerous world on the virtual or electronic front."[2]

– Candy Alexander, a Cybersecurity consultant, in 2015.

The hacking of Canada-based online dating website, Ashley Madison, in July 2015 left horrified subscribers facing a future of ruined reputations and relationships as blackmailers threatened to expose them unless they paid up. For instance, *"You got busted"* was the headline of a mail received by John R. (John), a 35-year-old member of Ashley Madison, in September 2015. The message continued, *"Unfortunately your data was leaked in the recent hacking of Ashley Madison and I know [sic] have your information. I have also used your user profile to find your Facebook page, using this I can now message all of your friends and family members."*[3] The letter demanded approximately US$500 to be paid within three days. Otherwise, according to the sender, John's friends and family would be informed of his Ashley Madison membership.

In July 2015, a team of computer data hackers, who called themselves 'The Impact Team' (Impact), sent a message to Avid Life Media Inc. (ALM) that they had stolen the customer records of their infidelity site Ashley Madison ***(Refer to Exhibit I for an image from Ashley Madison website and Exhibit II for the message from the Impact Team)***. The records consisted of customers' profiles and the company's financial records. ALM, a Toronto-based firm, owned Ashley Madison and related hook-up sites such as Cougar Life and Established Men. Impact sent a note to ALM saying it should shut down the Ashley Madison and Established Men websites immediately as they encouraged men and women to cheat on their partners by looking for extramarital relationships on the websites. They also threatened to release all the information about the subscribers of the websites online if ALM did not shut down those websites and did not give a deadline for doing so. The threat came as a bombshell to a lot of subscribers of these websites whose reputations and relationships would be in jeopardy if the hackers posted the information online.

As there was no response to their demand from ALM, Impact released a data dump which was 25 gigabytes in size in August 2015. This was accessible only through the Tor browser[a]. Later, the data was released through web search engines like trustify.com. The files included the email details, sexual preferences, physical descriptions, and log-in information of about 32 million users of Ashley Madison. Following this people like John started receiving threatening calls from blackmailers. The incident posed a dilemma to organizations worldwide on the credibility of cyber

[a] The TOR (third-generation onion routing) browser is a web browser designed for encrypted anonymous web surfing and protection against traffic analysis.

security in securing organizational data. Analysts opined that the hacking of the Ashley Madison website emphasized the need for organizations to have secure management information and data security systems. Marc Boroditsky, operating chief of Authy, a San Franciso-based security firm, said, *"Ashley Madison "is screwed" unless it takes swift action to tell members and investors: "This is what broke, this is how it broke it, and this is how we're going to fix it."*[4]

BACKGROUND NOTE

Online dating was a personal introductory system through which individuals could find and contact each other over the internet to arrange a date, usually with the objective of developing a personal, romantic, or sexual relationship[5]. Even before the advent of the internet, newspaper groups played host to a variety of dating activities like ads for match making. In addition to the forums created for posting personal ads, those who wanted a relationship with people with similar interests were meeting and getting to know others in forums of the print media. The internet began to be used for dating almost since its origin. Services such as Prodigy and America Online offered chat rooms and forums for singles and heavily advertised these features from 1985. The first major internet dating websites were kiss.com and match.com, which were both registered in 1994 and 1995 respectively. There were 16 dating websites listed on Yahoo![b] by 1996, and these included sites such as Friendfinder.com and OneandOnly.com.

Andrew Conru (Conru) created the first online dating site, webPersonals, in 1994. He sold it the following year. In 1996, he launched FriendFinder Networks Inc. (FriendFinder) and a social networking site called FriendFinder.com which was intended to help people connect with likeminded partners. Gradually, Conru found that people were posting naked pictures of themselves and looking for partners for adult-oriented activities. As a result, he started Adult FriendFinder in 1996. FriendFinder expanded its network by starting more dating sites like Senior FriendFinder, Amigos.com, BigChurch.com, and Alt.com.

Internet dating got a social boost with the release of the Hollywood movie "You've Got Mail" in 1998. The movie which starred Tom Hanks and Meg Ryan was about two business rivals who hated each other in person but fell in love over the web. Though the movie did not focus on internet dating directly, it painted a positive picture of meeting someone on the web and showcased the web as an instrument for bringing people together. The launch of Friendster and Myspace in 2002 brought in more changes in dating sites. It led to the inception of online "social networking" and some analysts felt that online dating was a by-product of social networking. According to a report from IBISWorld[c], the dating services industry, including online dating and offline matchmaking services, pulled in US$2.4 billion in annual revenue by 2015[6].

Ashley Madison was an infidelity website that facilitated discreet affairs for people who were looking for such affairs. Its tag line was 'Life is short. Have an affair'. The Ashley Madison site claimed to have more than 40 million members in 46 countries and was available in 28 different languages. It was launched in 2001 by Noel Biderman (Biderman), a Canadian internet entrepreneur. Biderman studied Economics at the University of California, and worked as a sports attorney and as an agent for athletes. According to a Bloomberg L.P[d] feature in 2011, Biderman's work as an agent involved helping professional basketball players cheat on their wives and mistresses. It was at this point that the idea for starting Ashley Madison took root in his mind.

---

[b] Yahoo Inc. is an American multinational technology company headquartered in Sunnyvale, California. It is globally known for its Web portal, search engine Yahoo! Search, and related services including Yahoo! Directory and Yahoo! Mail.

[c] IBISWorld is an Australian research organization specializing in long range forecasting of industries and the business environment with an emphasis on providing information for strategic planning and research purposes. IBISWorld's fiscal 2013 global revenue exceeded US$35 million.

[d] Bloomberg L.P is privately held financial software, data, and media company headquartered in New York. It maintains offices in more than 192 locations around the world.

Biderman was married with two kids. His wife, Amanda Biderman, appeared in interviews with her husband in which he discussed his adultery site but claimed that they were faithful to each other. Biderman showed no sign of any guilt about his role in enabling people to cheat on their partners through Ashley Madison. He described himself on his personal website as "the most hated man on the internet."

Ashley Madison was launched in 2001 and was acquired by Avid Life Media (ALM) in 2007, with Biderman leading the new company. ALM, founded in 2007, ran dating services through websites that targeted specific audiences who were looking for extramarital affairs. Its main brands were the websites AshleyMadison.com, CougarLife.com, and EstablishedMen.com. It also had a few brands like ManCrunch.com run by Established Men, SwapperNet.com, and TheBigandtheBeautiful.com, which were run by Cougar Life.

ASHLEY MADISON'S BUSINESS MODEL

Even though anybody could register on the Ashley Madison site for free, users who wanted to seek partners for relationships and to read and send messages had to pay a fee, which started at US$49. Ashley Madison worked based on the payment made by users to buy credits. The basic package was 100 credits for US$49. For 30 credits, a member got a 30-minute chat session with prospective partners. Premium customers who paid US$250 got a money-back *"affair guarantee"*. The website promised to pay back the money if the member did not have an affair within three months. The member, mostly the man, had to pay for five credits to initiate a conversation with another member, mostly a woman. The response from the other member was free and there the conversation started. The website had a chat facility in which women could send messages for free but men had to pay to read them. The site allowed users to hide their account profiles for free. If users wanted to permanently delete their accounts from the website, they had to pay US$19 and select the 'full delete' option. The 'full delete' option once chosen, removed the user profile, site usage history, messages sent and received, and the photos uploaded on the site.

Ashley Madison claimed that its users were 100% like-minded. It gave the assurance that the user's anonymity would be protected by its site security system and that its user registration details were kept private. It offered members a guarantee that it would help them to find a partner. It claimed on the website *"We guarantee that you will successfully find what you're looking for or we'll give you your money back".*[7] The site explicitly stated on its homepage that it was a destination for cheating wives and husbands who wanted to indulge in infidelity. *"Ashley Madison is the most famous name in infidelity and married dating,"* the site claimed on its homepage. It claimed, *"Have an Affair today on Ashley Madison. Thousands of cheating wives and cheating husbands signup everyday looking for an affair.... With our affair guarantee package we guarantee you will find the perfect affair partner."*[8]

In order to qualify for getting a partner, users had to purchase expensive packages on the site and send 'priority' messages to 18 unique members each month for three months. Apart from that, they had to send 5 Ashley Madison gifts per month and engage in 60 minutes of paid chat every month. ALM employed certain guerrilla marketing techniques to promote Ashley Madison. As part of this, it created a fake criticism website called www.AshleyMadisonScams.com. This was filled with advertisements of Ashley Madison and anonymous testimonies proclaiming that it was legitimate to join Ashley Madison. ALM advertised its dating sites through televisions, bill boards, and radio. The airing of most of these ads was, however, stopped in view of frequent complaints from members of the public who objected to the motive of the ads. Football stadiums and soccer teams rejected sponsorship offers from Ashley Madison. In 2009, NBC[e] refused an ad submitted

[e] The National Broadcasting Company (NBC) is an American commercial broadcast television and radio network owned by NBC Universal. NBC has eleven owned-and-operated stations and nearly 200 affiliates throughout the United States and its territories.

by Ashley Madison for broadcast during Super Bowl XLIII[f] in the US. Ashley Madison was known for the provocative promotional strategies it used to attract customers. It was even sued by the Queen of Spain in 2012 over a photoshopped picture of her in one of their advertisements. Such photos of Mitt Romney, Bill Clinton, and Prince Charles were also used in its ads.[9]

In January 2010, ALM attempted to go in for an IPO[g] on the Toronto Stock Exchange but was met with hesitation by investors due to the nature of its business. The plan was abandoned when the lead bank on the listing, GMP Securities LP[h], backed out after its chief executive analyzed in detail the nature of Ashley Madison's business. In April 2015, the company once again revealed plans to go in for an IPO on the London Stock Exchange. ALM said it planned to raise US$200 million in a London listing in April 2015. Analysts felt that the data breach by Impact in July 2015 had interrupted those plans. Avid Life spokesman Paul Keable said in this regard, *"It's far too early in the investigation to make any comment in relation to the impact on the business. To be honest, given the news of this week, our focus is obviously elsewhere."*[10] He continued saying, *"When and if we have news with regards to our business (IPO or otherwise), we will make the appropriate statements at that time."*[11]

Ashley Madison reportedly made US$115 million in 2014, a 45 percent increase from 2013. According to dailydot.com, ALM secretly operated an online escort service and actively engaged escorts for a separate dating website named escorts.ca aimed at "sugar daddies".[i] Escorts.ca was leased in 2013 through a shell company[j] called Pernimus Limited, which was listed among ALM's "legal entities" on an internal company memo. According to a leaked contract, ALM leased the escort-service property from an Ontario-based company called Steeltown Marketing Inc., on February 20, 2013[12]. The escorts.ca website was active until September1, 2015. After that, it was abruptly suspended.

BIG BLOW FROM THE IMPACT TEAM

On July 12, 2015, ALM employees arrived at work to find a message from Impact waiting for them. In that message, Impact stated that they had stolen the data of 37 million members of Ashley Madison. In the message, Impact said, *"Avid Life Media has been instructed to take Ashley Madison and Established Men offline permanently in all forms If ALM doesn't comply, we will release all customer records, including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails."*[13]

Impact also alleged that the 'full delete' option promised by ALM was not implemented by Ashley Madison as the data of users was actually never deleted from the Ashley Madison website. *"Full Delete netted ALM $1.7m in revenue in 2014. It's also a complete lie,"* the Impact Team wrote in a note posted online. *"Users almost always pay with credit card; their purchase details are not removed as promised, and include real name and address, which is of course the most important*

---

[f] Super Bowl XLIII was football game between the American Football Conference (AFC) champion Pittsburgh Steelers and the National Football Conference (NFC) champion Arizona Cardinals to decide the National Football League (NFL) champion for the 2008 season in the US.

[g] An initial public offering (IPO) or stock market launch is a type of public offering in which shares of stock in a company are sold to institutional investors that in turn sell them to the general public on a securities exchange, for the first time. Through this process, a private company transforms into a public company.

[h] GMP Securities is a leading independent investment dealer headquartered in Toronto, Canada, providing investment banking, institutional sales, and trading and research to a global client base that includes corporate clients and institutional investors.

[i] Sugar daddy is a term for a man who offers support (typically financial and material) to a younger companion, e.g. a kept woman.

[j] Shell companies are not necessarily illegal or illegitimate and can act as means of tax avoidance for legitimate businesses.

information the users want removed."[14] ALM denied this charge to a certain extent, saying in a statement that the 'full delete' process did what it claimed and involved *"a hard-delete of a requesting user's profile, including the removal of posted pictures and all messages sent to other system users' email boxes."*[15] The statement, however, did not speak about whether all traces of the customer's activity were removed from backend databases and logs, including the transaction records for requesting the deletion.

As the news of Ashley Madison data hacking spread virally through different media, users of the website began to panic about the possibility of their personal data being leaked online. ALM released a letter on July 20, 2015, to reassure its customers. In the letter, it said, *"We immediately launched a thorough investigation utilizing leading forensics experts and other security professionals to determine the origin, nature and scope of this incident."*[16] ***(Refer to Exhibit III for Avid Life Media's Letter to its Subscribers).*** In its response to the demand from Impact, ALM said it had adjusted its policy on deleting user data but gave no sign that it planned to close down the site. Though ALM claimed that it was erasing the data of users from the sites, analysts opined that the data could be recovered from somewhere on the internet as they felt that once data had been published on the internet, it would remain on the internet forever.

DATA LEAK BY IMPACT

Impact posted 25 gigabytes of user information online on August 18, 2015, as there was no reaction from ALM on its demand for the shutting down of the Ashley Madison and Established Men websites. The hacked information was released on BitTorrent[k] in the form of a 10 gigabyte compressed archive. The data included names, passwords, addresses, and phone numbers submitted by users of the site. The data dump also included descriptions of what the users were seeking in an affair partner. For instance, one member wrote, *"I'm looking for someone who isn't happy at home or just bored and looking for some excitement."*[17]

Initially, analysts had doubts about the legitimacy of the users' data but the credit card related information seemed to be genuine except for some members who used anonymous prepaid cards. But the credit card information was not enough for Impact to steal users' money. Ashley Madison made it clear that full credit card information was not leaked, saying, *"No current or past members full credit card numbers were stolen from Avid Life Media. Any statements to the contrary are false. Avid Life Media has never stored members full credit card numbers."*[18] ALM also assured its customers that it had increased the security of its networks. However, a second data dump occurred on August 20, 2015, which comprised 12.7 gigabytes of corporate emails, including Biderman's data.

The Ashley Madison hacking also revealed 197,000 emails from the inbox of Biderman. The leaked emails had a "selected dox" section which was a collection of documents, images, and other data from Biderman's inbox. It also included a 100-page movie script co-written by Biderman called *"In Bed with Ashley Madison."* The box had dozens of other sensitive documents, including a scan copy of Biderman's driver's license, copies of personal checks, bank account numbers, his income statements, and home address. Some of these emails referred to an app that the company was developing called "What's Your Wife Worth" ***(Refer to Exhibit IV Images from the "What's Your Wife Worth" App).*** The app allowed men to rate each other's wives in terms of monetary value. According to the emails, the ALM team was in the middle of developing the app in June 2013. In the emails, Biderman made a comment to Brian Offenheim, ALM's vice president of creative and design, and then approved Offenheim's design of the app's registration page. However, an email conversation of Biderman in February 2014 suggested that the app had been abandoned.

---

[k] BitTorrent is a protocol for the practice of peer-to-peer file sharing that is used to distribute large amounts of data over the Internet.

ALM started to investigate the data breach incident. It associated with the FBI[l], the Ontario Provincial Police, Toronto Police Services, and the Royal Canadian Mounted Police along with independent security experts, to investigate the Impact team. It announced a C$ 500,000 (US$ 377,000) cash prize for anyone who provided information leading to the identification, arrest, and prosecution of the persons accountable for the hack. ALM released a statement in August 2015 stating that it needed more help from outside in its efforts to catch the hackers. It said, *"The investigation is progressing in a 'positive direction,' but more help is needed from the outside. In the very best interest of our customers, who have been affected by this malicious act, we are firmly committed to fully assisting these law enforcement and investigative authorities, without reserve. Because of this active and ongoing investigation, there is little more we can provide at this time to the media and the public."*[19] Biderman claimed that the data hack had been done by someone who had had authentic access to the company's data in the past. *"We're on the doorstep of [confirming] who we believe is the culprit, and unfortunately that may have triggered this mass publication,"* Biderman told Krebsonsecurity[m]. He said, *"I've got their profile right in front of me, all their work credentials. It was definitely a person here that was not an employee but certainly had touched our technical services."*[20]

JITTERY SUBSCRIBERS

The hacking of Ashley Madison and the negative publicity surrounding the whole issue left a lot of existing and new customers of the site fearful. They felt that their existing relationships would be in trouble if their partners came to know that they had had an affair or had looked for an affair on Ashley Madison. Ashley Madison offered the 'full delete' option for free as a consolation measure to users. But analysts felt that if the hacked data was genuine, then the horse was already out of the barn and nobody could control data leaked on the internet. They pointed out that the hackers had given a chance to people with a grudge against others to defame them by spreading news of their involvement with Ashley Madison. For instance, some of the users worked in the US military. There were at least 13,000 addresses from military and government emails with .mil and .gov addresses. Committing adultery violated the Uniform Code of Military Justice in the US. It was a prosecutable offense that could result in these subscribers getting a year of imprisonment and a dishonorable discharge.

There were also more than 100 Vatican email addresses on the Pastebin.com[n] list where the hackers had posted a partial list of Ashley Madison users. If these were linked to the identity of priests, the users could be banished from the Catholic Church[21]. Some observers pointed out that though an individual's email or name was in the Ashley Madison database, it did not necessarily mean that person had an account. Since the site did not require users to verify their identity, many of the accounts were likely to be bogus. Security expert and blogger Robert Graham said, *"Obviously [some accounts are] made up things for people who just want to look at the site without creating a 'real' account."*[22] For instance, Tony Blair's email, tblair@labour.gov.uk, was exposed in the database, but this did not in any way mean that the former British prime minister had been using the site to find dates. UK public sector email addresses used on the site had been grouped into the following categories: education: ac.uk (1,716); government: gov.uk (124); MoD: mod.uk (92), local education authorities and schools: sch.uk (65); National Health Service: nhs.uk (56); police force; and police.uk (less than 50)[23].

Celia Walden, British writer and wife of television personality Piers Morgan, was also found to have registered with the site, but clarified that she had signed up as part of her research to prepare for an interview with Biderman. The official parliamentary email address of Israeli Knesset[o]

---

[l] The Federal Bureau of Investigation is the domestic intelligence and security service of the United States, which simultaneously serves as the nation's prime Federal law enforcement organization.

[m] KrebsOnSecurity is a daily blog which covers computer security and cybercrime.

[n] A website where users can store plain text and source codes.

[o] The Knesset is the name for Israel's parliament and is located in the capital, Jerusalem.

member Taleb Abu Arar was also listed, but the politician was quick to deny claims that he had used the website. *"[A hacker] signed up my email in order to damage my good name, and a complaint has been filed against the site, and the site which exposed the source of the registration,"*[24] he said.

The hacking also resulted in panic among gay subscribers. According to media reports, there were 79 countries where homosexuality was illegal. In Iran, Mauritania, Nigeria, Afghanistan, Qatar, Saudi Arabia, and the United Arab Emirates, the punishment for homosexuality was death. On social news site Reddit[p], one user claimed that he was a gay living in Saudi Arabia who had used the service under his own name to meet men in the US. He wrote, *"I am from a country where homosexuality carries the death penalty. I BEG you all to spread this message. Perhaps the hackers will take notice of it, and then, I can tell them to (at the very least) exercise discretion in their information dump (i.e. leave the single gay Arab guy out of it)."*[25]

John, who was threatened by the blackmailers, was so concerned that his data would be out as a member of Ashley Madison and that his wife would come to know, that he consulted New York-based reputation management firm Status Labs, which had set up a free hotline advising extortion victims of the Ashley Madison. John said, *"I didn't meet with any of them in person but I was tempted."*[26] He deleted his account in September 2014 after deciding to fix his marriage. Status Labs president Darius Fisher said, *"It's simple to switch your privacy settings, but it's important to remember that these extortionists, like all scammers and spammers, are playing a numbers game. If they scare even one or two people into paying up, it's a big payday for them."*[27]

Another revelation about the Ashley Madison hacking was that according to Associated Press[q], hundreds of US government employees from the White House, Congress, and law enforcement agencies had used internet connections in their federal offices to access the Ashley Madison website and to pay their membership fees ***(Refer to Exhibit V for Valid Ashley Madison Accounts Using Government Email Addresses Per Country).*** There were also employees from tech companies who had joined Ashley Madison ***(Refer to Exhibit VI for Number of Ashley Madison Accounts among the Largest Tech Companies).*** The hacked information posted by Impact was easily searchable on several websites. For instance, the www.haveibeenpwned.com site allowed users to enter an email address to know whether his/her profile had been leaked. Similarly, www.ashley.cynic.al and www.trustify.info/check sites allowed data to be checked by entering email addresses. However, ALM claimed that the "intellectual property in the data" was being infringed upon and ordered several sites to take down the service using Digital Millennium Copyright Act (DMCA)[r] requests. The US Police department also created a Twitter account @AMCaseTPS, and hashtag #AMCaseTPS urging the public to post any information related to Impact.

BOGUS FEMALE PROFILES

Impact alleged that thousands of the female profiles on Ashley Madison were fake. According to the media sources, 31 million male profiles were competing for 5.5 million women profiles in the database. But most of the women never chatted with anybody. Out of the total number of women profiles, only 2409 were engaged in chats. Analysts opined that the majority of men using Ashley

---

[p] Reddit is an entertainment, social networking, and news website where registered community members can submit content, such as text posts or direct links, making it essentially an online bulletin board system.

[q] The Associated Press (AP) is an American multinational non-profit news agency headquartered in New York. It operates 243 news bureaus in 120 countries.

[r] The Digital Millennium Copyright Act (DMCA) is legislation enacted by the United States Congress in October 1998 which strengthens the legal protection of intellectual property rights in the wake of emerging new information communication technologies, i.e., the internet.

Madison were not having any affairs. Actually, most of them were chatting with bots[s] and administrators instead of chatting with real women and they were paying a lot of money for this. These bots were programmed with automated replies created by technical people at Ashley Madison. Most of the bots accounts used the ashleymadison.com email address because, in comparison to men, a very small number of women signed up on the site. These bots would supposedly send messages to millions of members, creating an illusion that they were contacting them directly with the aim of arranging a sexual relationship. This prompted two lawsuits against Ashley Madison in California and Maryland by men who felt they had been intentionally cheated.

A former employee of Ashley Madison, Doriana Silva from Canada, sued ALM in 2012 claiming around US$20 million in damages. She claimed that she had gotten repetitive stress injuries in her hands after the company appointed her to create 1,000 fake profiles of women in Portuguese over three months. She claimed these profiles were targeted at a Brazilian audience. ALM countersued Silva, saying she had retained copies of confidential documents including copies of her work product and training materials. The suit by ALM sought to recover the documents as well as US$100,000 in damages plus legal costs. The case was settled out of court, but ALM continued to maintain that Silva had never made any fake profiles. The evidence, however, suggested that ALM's statement was false. According to Gizmodo[t], many of the email addresses used by these fake accounts were created with the extension @ashleymadison.com and seemed to have been generated by robots.

Gizmodo analyzed email addresses, IP addresses, and the last time female users had checked the messages in their Ashley Madison inbox to look for signs of human life. The data showed that only about 9,700 women had ever replied to a message (compared to 5.9 million men) and about 2,400 had used the chat system (compared to 11 million men)[28]. According to the media sources, a member of the site, David Poyet, sued Ashley Madison in October 2015 for US$5 million in damages, claiming the site *"went to extreme measures to fraudulently lure in and profit from customers,"* including *"creating over 70,000 female bots to send male users millions of fake messages."*[29] Annalee Newlitz from Gizmodo wrote, *"Ashley Madison is a site where tens of millions of men write mail, chat, and spend money for women who aren't there."*[30]

THE HACK AFTERMATH

The Ashley Madison hacking resulted in chaos in different sections of society. If reports were to be believed, two persons committed suicide after their details were leaked online. One was Captain Michael Gorhum, who had worked for 25 years with the San Antonio Police Department in Texas. His death came just days after his official email address was linked to an Ashley Madison account. Canadian police confirmed the second suicide in August 2015. This was also believed to be that of an Ashley Madison subscriber. Another high-profile victim was Jeff Ashton, State Attorney for Orange and Osceola counties in Florida, who resigned from his post after it was revealed that he was an Ashley Madison user.

According to NBC News[u], at least five lawsuits were filed against Ashley Madison in Canada and in US courts in California, Texas, and Missouri. Charney Lawyers and Sutts and Strosberg LLP, which were Canadian law firms, filed a class-action lawsuit[v] against Ashley Madison in August 2015 for US$578 million on behalf of Canadians whose information had been leaked online. The

---

[s] An Internet bot, also known as web robot is a software application that runs automated tasks over the Internet.

[t] Gizmodo is a design and technology blog. It is part of the Gawker Media network run by Nick Denton.

[u] NBC News is a division of the American broadcast network NBC. The division presides over America's number-one-rated newscast, NBC Nightly News, and the longest-running television series in American history, "Meet the Press with Chuck Todd".

[v] A class action lawsuit is one in which a group of people with the same or similar injuries caused by the same product or action sue the defendant as a group.

plaintiff in this case was Canadian widower Eliot Shore, who had joined Ashley Madison after his wife of 30 years died of cancer. Eliot Shore, whose details were published on the internet, had described himself as a disabled widower from Ottawa on the website and he also sued Ashley Madison for US$7.65 million in punitive damages[w]. According to the lawyers, the lawsuit alleged that Ashley Madison had failed to protect the information of users like personal names, emails, home addresses, and message history.

The analysis of the leaked data showed that the passwords of the members had been stored on a database after they were protected using a process known as hashed form, a common security practice using a cryptographic function called bcrypt. These scrambled passwords made it hard to carry out "brute force attacks"[x] that tried a lot of different word and letter combinations because hashing with bcrypt secured the database. As a consequence, a brute force attack on the passwords would take years. The procedure was not supposed to be changed unless the algorithm was defective. However, a password cracking team called Cynosure Prime, after analyzing the leaked data of Ashley Madison, acknowledged that at some point the Ashley Madison site had changed the way passwords were stored. This change had removed the protection bcrypt afforded to the passwords database. Cynosure Prime cracked the 11 million passwords in about 11 days in October 2015. According to a London-based security consultant, Gabor Szathmari, ALM had failed to use either CAPTCHAs[y] or email verification to find out bots during the account creation process. He said, *"End result of sensitive data stored in the source code repos is a much more vulnerable infrastructure. Database credentials, AWS tokens probably made the lateral movement easier for the Impact Team, leading to the full breach of Ashley."*[31]

Analysts said Impact's demand was not for financial benefit but was an expression of a moral outrage. They also opined that the mere fact that a person's data was included in the leak did not mean that they had used the site to have an affair. Tod Beardsley of information security firm Rapid 7 said, *"It's trivial to set up a fake account on Ashley Madison, since Avid Life Media's account setup procedures encourages, but does not require, an e-mail address to be verified by the user. The majority of 'real' account holders tend to use fake, throw-away data and details, for obvious reasons. Even if the real data is a real person, and that person really registered for the site, there is no indication in the data if that person was successful at, or even intending to, pursue an illicit affair."*[32]

ASHLEY MADISON WAS NOT THE FIRST...

According to industry experts, 2014 was one of the worst years on record for data breaches in the US, with nearly 350 million records lost or stolen. [33] While only the most high profile cases were reported in the media, small and medium enterprises (SMEs) were at high risk. According to a McAfee report released in 2014, almost 90% of small and medium-sized businesses in the US did not use data protection for company and customer information.[34] A Kaspersky Lab survey in the same year in 2014 revealed that 75% of SMEs believed that their business was too small to be attractive to cyber criminals, while 59% felt that the information they held was not of interest to cyber criminals.[35]

Data breaches followed in 2015 and Ashley Madison was not the first victim. A similar incident happened in April 2015 with Adult FriendFinder. Adult FriendFinder had more than 40 million members, according to its website. FriendFinder claimed that it had more than 600 million registered users across some 40,000 websites in its network. A Thai hacker using the name

---

[w] Punitive damage is the monetary compensation awarded to an injured party that goes beyond the compensation for the individual for losses and is intended to punish the defendant.

[x] Brute Force Attack refers to the attempts which aim at gaining access to a site and it tries usernames and passwords, over and over again, until it gets in.

[y] A CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) is a type of challenge-response test used in computing to determine whether or not the user is human.

ROR[RG] claimed responsibility for the breach, and demanded a US$100,000 payment to avoid more leaks of data stolen from the site. Several members had registered on Adult FriendFinder using their work email addresses, including the email addresses for the U.S. Army, U.S. Air Force, Australian military, Brazilian military, Canadian military, and Colombian military, as well as several international government addresses. FriendFinder mentioned that it had hired FireEye's forensics unit, Mandiant, to investigate along with Holland and Knight, a law firm cum public relations enterprise specializing in cybersecurity.

Earlier, Sony Corporation[z] (Sony) also came under attack from hackers who called themselves 'Guardians of Peace' on November 24, 2014. The hackers had reportedly obtained 100 terabytes of data from Sony servers. Film budgets and confidential contracts, and the user names and passwords of Sony executives were also included in the stolen data. Following this, Sony shut down all computer systems, including those in its overseas offices. It even debated whether to take Sony Pictures entirely offline to prevent any further damage. As a result of the hacking, five Sony films, including four that were yet to be released, were put on online file sharing hubs. Brad Pitt's *Fury*, which had already been released in theaters, was illegally downloaded more than 1 million times within a week. *Annie*, *Mr. Turner*, *Still Alice*, and *To Write Love on Her Arms*, all of which had not yet been released in theaters, were also being downloaded. Sony suspected that North Korea might be responsible for the attack in vengeance for *'The Interview'*, a comedy movie about a clumsy plot to murder North Korean dictator Kim Jong-un. A North Korean website had called the movie as an 'evil act of provocation'. On December 1, 2014, the pre bonus salaries of the top 17 Sony executives were leaked. The files also contained the salaries of more than 6,000 current and former Sony employees. In a major embarrassment for Sony, emails were leaked, some of which revealed a Sony official's embarrassing gossip about celebrities and racist jokes made against US President Barack Obama.[36] While North Korea denied any connection with the hacking, the FBI confirmed publicly that the government of North Korea was behind the Sony hacking.

THE ROAD AHEAD

Analysts opined that Ashley Madison seemed to be out of danger from the consequences of lawsuits due to the terms and conditions it had laid down on the site which had to be accepted by the members before they logged in. Ashley Madison had made several direct and bold disclaimers, which in summary stated:

- Use our site, and it's not our problem if your data gets hacked.
- If you use our site, we are not liable for damages, and if we are, you can't sue us for more than US$5,000.
- You may be interacting with fembots and not actual human beings seeking to have affairs.
- If you sue us, you must do it via arbitration and you may not do it as part of a class action lawsuit.[37]

Analysts also opined that the Ashley Madison data hacking issue raised a debate over the safety of online transactions as well as the need for installing a vigilant data security system in organizations. They felt that organizations needed to have a strong and secure management information system which prevented data breach by third parties. However, users who wanted to date online should be careful with their credentials in future in light of the Ashley Madison episode. Shayne Veramallay, who frequently searched dating websites for a partner said, *"Ashley Madison was kind of eye opening. It shed light on a lot of issues I face with online dating. You never know who's on the other end."*[38]

---

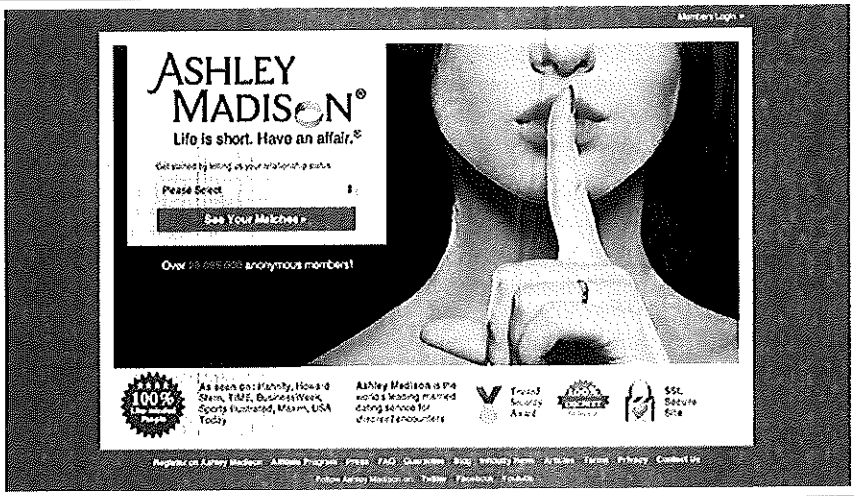
[z] Sony Corporation is a Japanese multinational conglomerate corporation headquartered in Tokyo, Japan. Sony is ranked 116th on the 2015 list of Fortune Global 500.

As a consequence of the data breach at Ashley Madison, Biderman stepped down from his post at ALM in August 2015. ALM was to be led by "an existing senior management team" until a new CEO was appointed, and it would continue to work with law enforcement in pursuit of the hackers, the company said. Despite the hack issue giving it negative publicity, Ashley Madison claimed on August 24, 2015, that new users were joining to use its service. The site released a statement claiming, *"This past week alone, hundreds of thousands of new users signed up for the Ashley Madison platform including 87,596 women."*[39] However, the company had to still deal with a number of lawsuits due to the hacking incident and its business practices.

When even the world's most trusted corporations like Sony were not perfect in terms of data security, it was no wonder that consumers were worried about cyber security. Analysts opined that as credit card details, passwords, and personal information were at the stake, every organization had to pay the utmost attention to the installation of secure management information and data security systems – something which many organizations in fact neglected to do. Analysts opined that Ashley Madison had the big responsibility of gaining back the confidence of its members as well as of the public by coming out with a revival strategy for its future existence.

Exhibit I

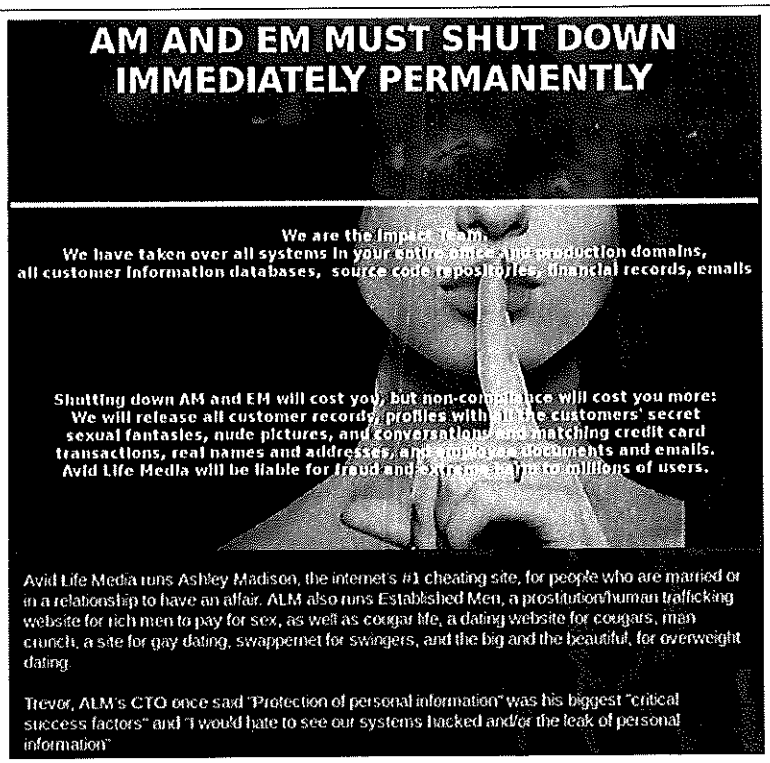
An Image from Ashley Madison Website



Source: www.ksl.com/?nid=151&sid=35580017

Exhibit II

Message from the Impact Team to Ashley Madison



Source: www.computerworld.com/article/2949980/cybercrime-hacking/extramarital-affairs-may-not-have-been-secrets-even-before-ashley-madison-hack.html

Exhibit III

Avid Life Media's Letter to its Subscribers following the Hack of Data by The Impact Team

TORONTO, July 20, 2015 /PRNewswire/ -- We were recently made aware of an attempt by an unauthorized party to gain access to our systems. We immediately launched a thorough investigation utilizing leading forensics experts and other security professionals to determine the origin, nature, and scope of this incident.

We apologize for this unprovoked and criminal intrusion into our customers' information. The current business world has proven to be one in which no company's online assets are safe from cyber-vandalism, with Avid Life Media being only the latest among many companies to have been attacked, despite investing in the latest privacy and security technologies.

We have always had the confidentiality of our customers' information foremost in our minds, and have had stringent security measures in place, including working with leading IT vendors from around the world. As other companies have experienced, these security measures have unfortunately not prevented this attack to our system.

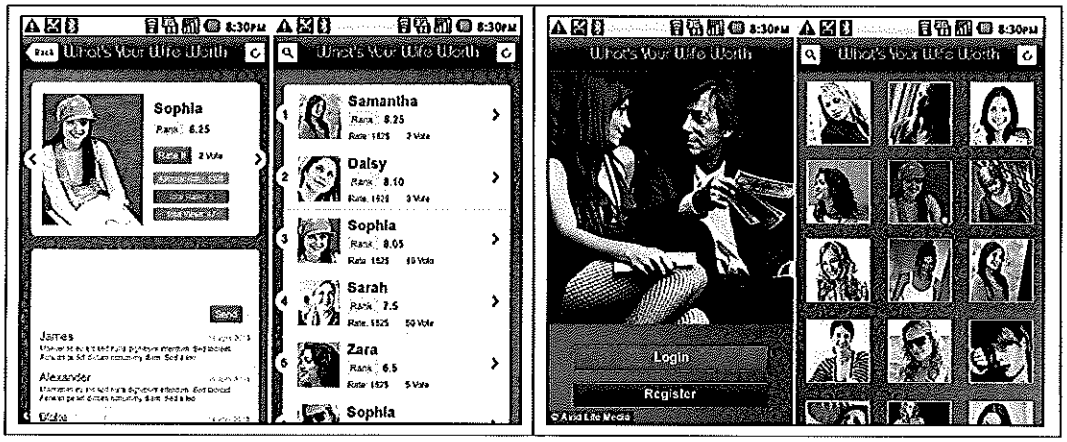
At this time, we have been able to secure our sites, and close the unauthorized access points. We are working with law enforcement agencies, which are investigating this criminal act. Any and all parties responsible for this act of cyber–terrorism will be held responsible.

Avid Life Media has the utmost confidence in its business, and with the support of leading experts in IT security, including Joel Eriksson, CTO, Cycura, we will continue to be a leader in the services we provide. "I have worked with leading companies around the world to secure their businesses. I have no doubt, based on the work I and my company are doing, Avid Life Media will continue to be a strong, secure business," Eriksson said.

Source: www.prnewswire.com/news-releases/statement-from-avid-life-media---august-28-2015-300134655.html

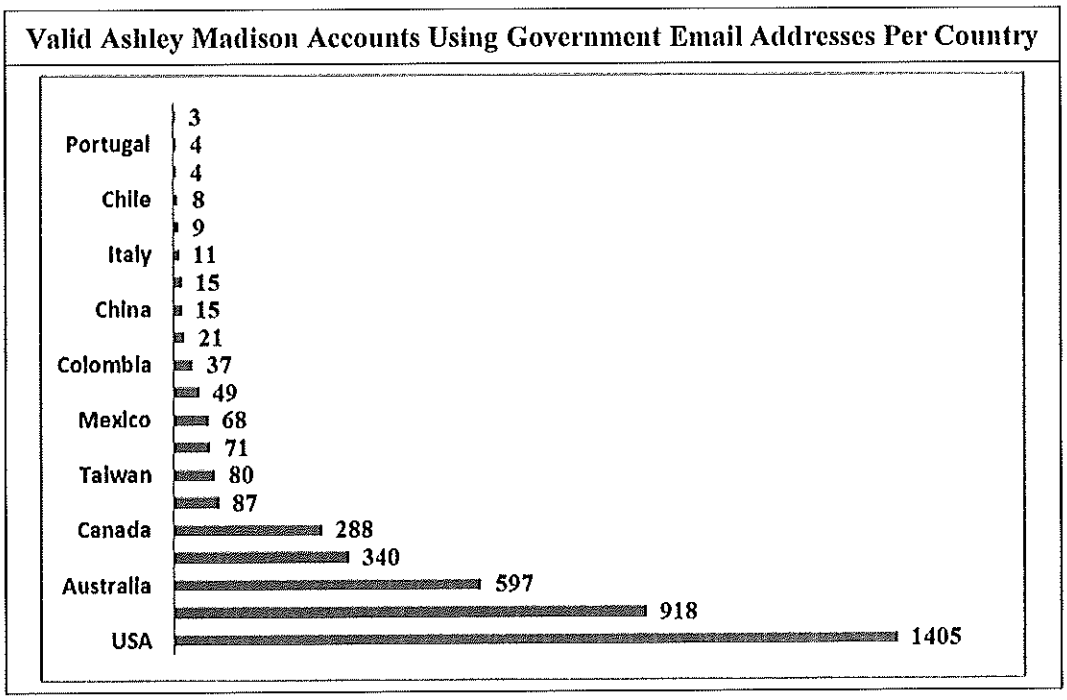
Exhibit IV

Images from the "What's Your Wife Worth" App



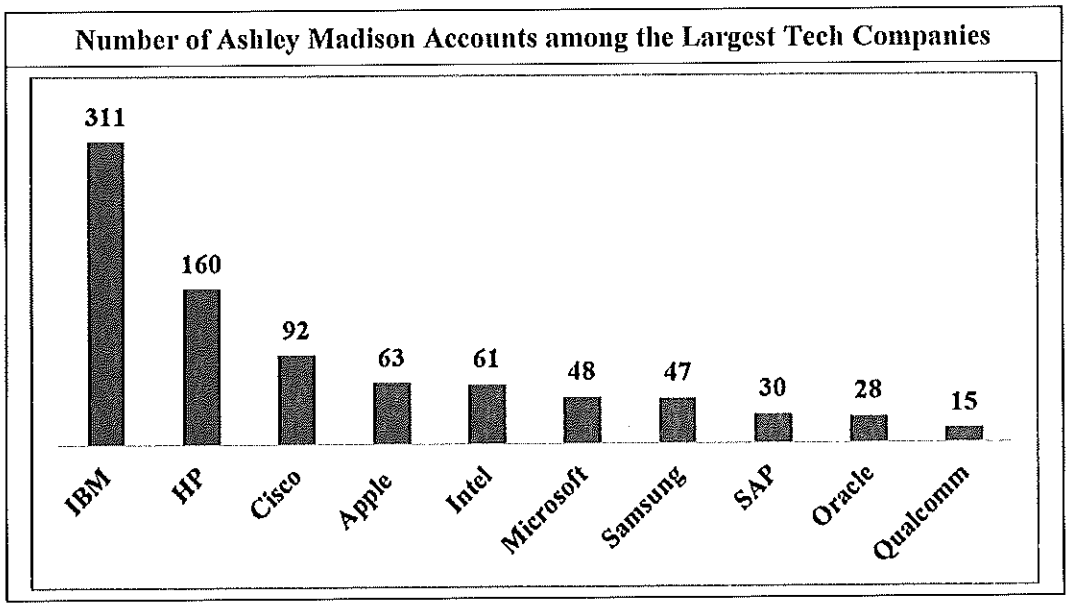
Source: www.dailymail.co.uk/sciencetech/article-3213300/Ashley-Madison-developing-s-Wife-Worth-app-gave-women-site-rating-dollar-value.html

Exhibit V



Source from http://dadaviz.com/s/ashley-madison-revealed

Exhibit VI



Adapted from http://dadaviz.com/s/ashley-madison-revealed

End Notes:

[1] John McAfee, "John McAfee: Why the Hacking of Ashley Madison Will Go Down in History," www.digitaltrends.com, November 10, 2015.

[2] David Weldon, "Ashley Madison Breach Shows Hackers May be Getting Personal," www.cio.com, September 30, 2015.

[3] Jane Ridley, "The Storm isn't over yet for Ashley Madison Cheaters," www.nypost.com, October 29, 2015.

[4] James Covert, "Is Ashley Madison IPO Doomed Because Of Leak?" www.nypost.com, August 19, 2015.

[5] www.en.wikipedia.org/wiki/Online_dating_service.

[6] Claire Brownell, "Ashley Madison Hack a Cautionary Tale in the Digital Hook-up World: 'They've Failed at a Key Value'," www.business.financialpost.com, July 20, 2015.

[7] "Is Ashley Madison a Scam? Is Ashley Madison a Fraud?" www.ashleymadison.com, August 17, 2014.

[8] Kim Zetter, "Hackers Finally Post Stolen Ashley Madison Data," www.wired.com, August 18, 2015.

[9] Rob Price, "The Strange Rise and Sudden Fall of Noel Biderman, the Former CEO of Ashley Madison," www.businessinsider.in, August 28, 2015.

[10] Kristen Schweizer, Ruth David and Scott Deveau, "AshleyMadison.com's second attempt at an IPO looking increasingly unlikely," www.business.financialpost.com, July 22, 2015.

[11] James Covert, "Is Ashley Madison IPO Doomed Because Of Leak?" www.nypost.com, August 19, 2015.

[12] Dell Cameron, "Ashley Madison's Parent Company Secretly Operated an Escort Website," www.dailydot.com, September 2, 2015.

[13] Timothy B. Lee, "The Ashley Madison Hack, Explained," www.vox.com, August 19, 2015.

[14] Graham Lanktree, "Ashley Madison Hack: Data for Removed Profiles 'Remains in Leaked Database' Despite $19 Delete Fee," www.ibtimes.co.uk, August 20, 2015.

[15] Kim Zetter, "Answers to Your Burning Questions on the Ashley Madison Hack," www.wired.com, August 21, 2015.

[16] Kim Zetter, "Hackers Finally Post Stolen Ashley Madison Data," www.wired.com, August 18, 2015.

[17] Maureen O'Neill, "Secrets and Lies: Corporate Data Security Lessons from the Ashley Madison Hack," www.metrocorpcounsel.com, October 14, 2015.

[18] Alex Hern, "Ashley Madison Hack: Your Questions Answered," www.theguardian.com, August 20, 2015.

[19] Alyssa Newcomb, "Ashley Madison Hack: The Latest on the Police Investigation," www.abcnews.go.com, August 24, 2015.

[20] Geoffrey Smith, "Hackers have Got All of Online Adultery Site Ashley Madison's Data," www.fortune.com, July 20, 2015.

[21] "How the Ashley Madison Hack Could Threaten People's Lives," www.news.vice.com, August 21, 2015.

[22] "How the Ashley Madison Hack Could Threaten People's Lives," www.news.vice.com, August 21, 2015.

[23] Lewis Dean, "Ashley Madison Hack Celebrities Named: Which Well-Known Figures Were Signed Up To The Adultery Website?" www.ibtimes.co.uk, August 20, 2015.

[24] Lewis Dean, "Ashley Madison Hack Celebrities Named: Which Well-Known Figures Were Signed Up To The Adultery Website?" www.ibtimes.co.uk, August 20, 2015.

[25] Sam Thielman, "Top Data Security Expert Fears Traumatic Aftermath in Ashley Madison Hack," www.theguardian.com, August 19, 2015.

[26] Jane Ridley, "Extortion Threats Are Being Made against People Who Were on Ashley Madison," www.news.com.au, October 30, 2015.

[27] Jane Ridley, "Extortion Threats Are Being Made against People Who Were on Ashley Madison," www.news.com.au, October 30, 2015.

[28] Claire Brownell, "Ashley Madison's Female Users Are Pretty Much Non-Existent, Evidence Shows," www.business.financialpost.com, August 27, 2015.

[29] Arden Dier, "Guy Sues Ashley Madison Over "Army of Fembots"," www.newser.com, November 2, 2015.

[30] Matt Rosoff, "Ashley Madison Was a Bunch of Dudes Talking to Each Other, Data Analysis Suggest," www.businessinsider.in, August 27, 2015.

[31] Rene Millman, "Ashley Madison's Source Code Reveals Poor Security Practices," www.scmagazineuk.com, September 9, 2015.

[32] Alex Hern, "Ashley Madison Hack: Your Questions Answered," www.theguardian.com, August 20, 2015.

[33] James Warren, "Why US Small Businesses Should Worry about Cybersecurity and How to Act," www.itgovernanceusa.com, February 12, 2015.

[34] "Your Secret's Safe with No One: Lessons Learned from the Ashley Madison Hack," www.scriptrock.com, 2015.

[35] James Warren, "Why US Small Businesses Should Worry about Cybersecurity and How to Act," www.itgovernanceusa.com, February 12, 2015.

[36] Bruce Schneier, "Lesson from the Ashley Madison Hack: Cloud Makes Everyone Vulnerable," www.nextgov.com, September 9, 2015.

[37] Brian Powers, "Ashley Madison's Online Terms and Conditions May Leave It Legally Undressed," www.forbes.com, October 22, 2015.

[38] Abby Ellin, "After Ashley Madison Breach, Online Daters Check Credentials," www.nytimes.com, October 15, 2015.

[39] Jonathan Chew, "Ashley Madison: Site Is 'Still Growing,' Despite Hack," www.fortune.com, August 31, 2015.