AFTER THE BREACH:
Analyzing Hacks of the Past

BP NETWORK

INTRODUCTION

The dark web. It sounds like the name of a deep-sea trench straight out of James Cameron's Sci-Fi classic The Abyss. In reality, this is a nocturnal void of the Internet where illegal activities fester. The dark web is submerged, hidden from search engines like Google, and it is where stolen data goes to be mined for profit.

Often, this data never re-surfaces again. As Business Insider described, these are the "dark alleyways" of the internet.[1] Imagine your corporate data disappearing down this dark path. Unfortunately, this is a regular nightmare scenario for decision-makers of some of the largest companies in the world.

No one is safe from being hacked. 174 breaches occurred the first 3 months of 2015, according to Forbes.[2] Those breaches alone affected 100 million customer records.
Some of the most notorious network security hacks have made headlines, and there are lessons to learn from those cautionary tales. Understand the miss-steps of these companies, and you can better prepare and potentially prevent the next large-scale breach from erupting.

In this eBook, we will not only reveal 10 hacks that rocked the IT security world, but we'll tell you how these hacks could have been stopped before they ever started...before entering the dark web.

ASHLEY MADISON

WHAT HAPPENED:

32 million users of the social networking site – which promotes infidelity and affairs between married individuals – had their personal information hacked. In addition, company financial records were also compromised. The hackers threatened to expose all of this information if the Ashley Madison website wasn't taken down.

THE BLOODY AFTERMATH:

Using the dark web, hackers made good on their threat and have already exposed 9.7 gigabytes of personal user data– including account details, log-in information, email addresses, and credit card payment transactions.[3]

LESSONS LEARNED:

According to Noel Biderman, the Chief Executive of Avid Life Media (the company that owns Ashley Madison), the hack had the markings of an inside job. Although he didn't go so far as to identify a former employee as the culprit, he confirmed that the person had access to their systems.

"I've got their profile right in front of me, all their work credentials," explained Biderman. "It was definitely a person here that was not an employee but certainly had touched our technical services."[4]

Inside attacks are often the most difficult to block. According to a global survey conducted in the 2015 Vormetric Insider Threat Report, 89% of organizations feel at least somewhat vulnerable to insider attacks, while 34% feel very or extremely vulnerable.[5]

WHAT YOUR COMPANY CAN DO:

Tier privileges and establish strict access controls. Users should have to build a certain level of trust before begin given privileged access to information. Also, establishing an audit trail is equally important to confirm that authorized steps were taken by users accessing data.

HOME DEPOT

WHAT HAPPENED:

This home-improvement franchise suffered a large-scale data breach, in which 56 million credit and debit card numbers were stolen. The attack occurred at various payment terminals across all nationwide Home Depot locations. 53 million customer email addresses were also lifted.

THE BLOODY AFTERMATH:

The 56 million stolen cards were put up for sale immediately on dark web channels. The hackers of this operation are believed to be from the same underground affiliate responsible for data breaches against Target, Sally Beauty, and P.F. Chang's.

LESSONS LEARNED:

According to Krebs on Security, there were several points of vulnerabilities that hackers penetrated within this intricate breach.[6] Hackers were able to access the perimeter of Home Depot's network by stealing a third-party vendor's user name and password credentials. They also took advantage of a security gap in Microsoft Windows that wasn't patched before the breach occurred.

WHAT YOUR COMPANY CAN DO:

Keep up-to-date on security patches.

Lack of patching is a common stumbling block for organizations. Some organizations don't update their patches for years. However, systems that run unpatched software are often the easiest forms of prey for hackers.

The U.S. Computer Emergency Readiness Team (CERT) explained the importance of preventative patch management: "The longer a system remains unpatched, the more vulnerable it is to being compromised. Timely patching is one of the lowest costs, yet one of the most effective steps, that an organization can take to minimize exposure to the threats facing its network."[7]

ANTHEM

WHAT HAPPENED:

The second-largest health insurer in the nation experienced the largest medical-related cyber intrusion in history. 80 million current and former members/employees of Anthem were hacked, resulting in the exposure of their private data.

THE BLOODY AFTERMATH:

This breach didn't involve private health records or credit card numbers. Instead, Social Security numbers, income details, email addresses, and other private information were made available on the black market.

As detailed in the Washington Post, the hackers could use this information to leverage more privileged medical information.[8] But as of yet, there has been no confirmation that the specific information in question has been used for suspicious or threatening activities.

The data breach is being linked to the Chinese government and Chinese government-sponsored entities, including researchers.[9] The FBI has been in the process of connecting the same dots, while the organization ThreatConnect matched up the patterns between the malware used in the Anthem attack with the malware used in the breach of a small U.S. defense contractor.

LESSONS LEARNED:

Lack of encryption led to a storming of the gates. Specifically, Anthem failed to encrypt the Social Security numbers of its customers. The reason? Anthem also wanted the integrity of that information preserved so it would be easier to pull unique health care trends to share with health care providers.

According to the Wall Street Journal, Anthem also believes that the hackers used stolen employee password information to gain access to the database.[10] Had the information been encrypted, the hackers would have had a tougher time descrambling the data and breaking through.

WHAT YOUR COMPANY CAN DO:

Use data encryption and multi-factor authentication.

JP MORGAN CHASE

WHAT HAPPENED:

The data breach of one of the largest banks in the nation, JPMorgan Chase, compromised the accounts of 76 million households and 7 million small businesses. No data was knowingly stolen, however.

THE BLOODY AFTERMATH:

The digital hack that intruders performed resembled the robbing of a physical bank vault. The master thieves were able to get their hands on a list of all the applications and systems that run on JPMorgan's computers, much like the floor plans of a bank. They were then able to pinpoint the common vulnerabilities in these programs and applications.

Fortunately, the breach was detected before the intruders ever stole any of the privileged financial information.

LESSONS LEARNED:

The ultimate downfall of JPMorgan's defenses came down to similar factors that tripped-up Home Depot.[11] The main point of entry was a server that lacked a two-factor authentication process. Evidently, the company does use two-factor authentication for their other systems, but dropped the ball in this instance, thus showing that even a single server can be a launch pad for criminal activity.

In addition, the hackers stole the credentials of a JPMorgan employee – a common theme in these breaches.

WHAT YOUR COMPANY CAN DO:

Implement comprehensive two-factor authentication processes, network segmentation, and demanding access-management policies within your data center.

As Computer World recommends, these protection measures can help prevent hackers from inflicting damage once they get into the network. But, it's a tall task to establish universal polices across the vast terrain of networks and systems.

TARGET

WHAT HAPPENED:

Target experienced a data breach that can safely be characterized as cataclysmic. More than 110 million of their customers had their personal and financial information ripped away from them by malware-infected point-of-sale (POS) systems at checkout counters.

THE BLOODY AFTERMATH:

Target is paying a hefty price for this breach. According to NBC News, Target reached a settlement with Visa "to fund up to $67 million in pre-tax payments to Visa and the financial institutions that issued the cards."[12]

This settlement follows another settlement that was reached with MasterCard in which Target must pay back $20 million for damages.[13]

LESSONS LEARNED:

The Target hack can be traced back to a third-party vendor employee who carelessly opened an infected email. As Krebs on Security described, "[the breach] appears to have begun with a malware-laced email phishing attack sent to employees at an HVAC firm."[14] The theft of credentials took place approximately two months before hackers went in for the kill to steal credit card data from Target cash registers.

Hackers devised a devious scheme to crack open Target POS checkout devices by using a type of memory-scraping malware. Specifically, the malware pulled information from data that still remained in the checkout systems' memory, after credit card swipes went through.

The Target and Home Depot breaches have some eerie similarities. In both instances, a third-party's hacked information sparked a cybersecurity wildfire. And, in both cases, self-checkout systems were targeted.

What Your Company Can Do:

Teach your employees how to detect phishing emails. Companies are only as strong as their weakest entry point and user, after all. Vigilant protection is necessary at all times.

EBAY

WHAT HAPPENED:

145 million active eBay users were asked to change their passwords as a preventative measure. This was necessary when hackers stole encrypted passwords and other personal user information, such as names, e-mail addresses, physical addresses, phone numbers, and dates of birth.

THE BLOODY AFTERMATH:

In the wake of this security breach, eBay faces a class action lawsuit filed by a Louisiana resident named Collin Green.[15] Despite the fact that no financial information was found to be compromised, the consumer privacy lawsuit cites a failure to protect the identify information of millions of eBay's customers.

LESSONS LEARNED:

eBay released a statement explaining that a small number of employee log-in credentials were hacked into, prompting their request to change passwords. According to Amanda Miller, a spokesperson for eBay, the incident wasn't discovered for about a month. It then wasn't revealed to the public until a few weeks later.[16]

But how did the cyber criminals manage to gain access to eBay's network? The details, at this point, have yet to be revealed. SC Magazine has speculated that a phishing attack could have been in play. There is also a possibility that a different form of social engineering was used to dupe an unsuspecting employee to click an infected e-mail link.[17]

What Your Company Can Do:

Regardless of what form of attack was employed, SC Magazine recommends establishing a defense strategy at multiple infrastructure layers, including the server layer, software layer, the file layer, web browser layer, and network layer. [18]

PREMERA

WHAT HAPPENED:

A nasty cyberattack exposed the medical and financial information of 11 million customers. The various types of financial and medical data that were pillaged include banking account numbers, Social Security numbers, and birth dates.

THE BLOODY AFTERMATH:

The Seattle Times reported that the health insurer is facing 5 class-action lawsuits that have been filed in the Seattle branch of the U.S. District Court on behalf of customers located in Washington, Nevada, and Massachusetts.[19] The complaints include negligence, breach of contract, violation of the Washington Consumer Protection Act, and failure to disclose the breach in a timely manner.

LESSONS LEARNED:

According to Dave Kennedy (a chief executive of TrustedSEC), medical records can be a big draw on the black market.[20] “Medical records paint a really personal picture of somebody’s life and medical procedures,” explained Mr. Kennedy. “They allow you to perpetrate really in-depth medical fraud.”

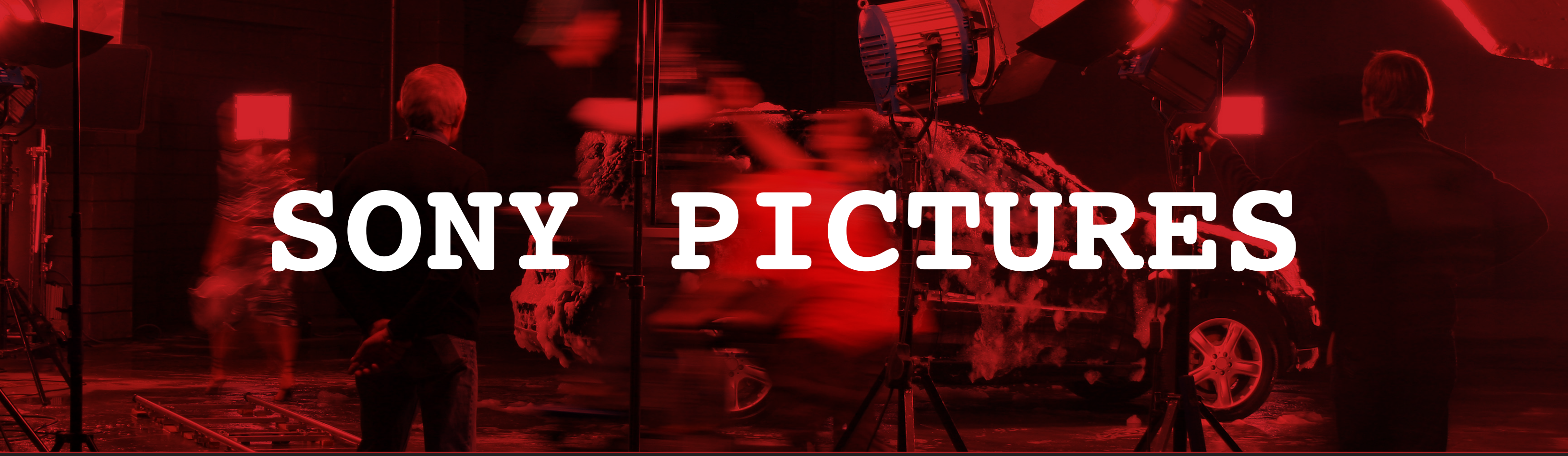
Medical fraud is easier to commit with information that is highly confidential. After all, that type of information is more heavily guarded and rarely sees the light of day.

If it does see the light, the ramifications can be fraudulent medical procedures that add up to large-scale medical and healthcare costs. However, Premera has yet to confirm that the breached data has been misused.

It is unclear the absolute cause for the Premera breach, but reports stated that a “suspicious domain called ‘prennera.com’ may have been spoofing Premera’s official website.”[21] This faux website went live in December 2013.

What Your Company Can Do:

Regardless of what form of attack was employed, SC Magazine recommends establishing a defense strategy at multiple infrastructure layers, including the server layer, software layer, the file layer, web browser layer, and network layer. [18]



SONY PICTURES

WHAT HAPPENED:

40 GB of leaked internal data was made public, impacting 6,800 global employees and 3,500 members of the Sony U.S. staff. The type of information that was leaked ranged from unreleased TV show pilots to salaries, criminal background checks, medical absence notes, and more.

THE BLOODY AFTERMATH:

The hackers made the information public on different file-sharing sites after sending a warning to Sony. This led to further embarrassment and indecent exposure for Sony employees, leaders, and all associated parties involved.

Calling themselves the Guardians of Peace (GOP), this group of data abductors leaked five unreleased Sony films, leading to a financial hit at the box office. On a larger level, Sony's reputation has taken the biggest hit of all.

LESSONS LEARNED:

The FBI has drawn links between the GOP and North Korea. In fact, the prevailing thought is that North Korea committed the hack against Sony in retaliation for the release of The Interview.

The Interview, of course, is the movie Seth Rogan and James Franco stared in about an assassination attempt on Kim Jung Un. The hack didn't deter Sony from releasing The Interview. They just pushed back the Christmas release date.

According to Forbes (which called this "the hack of the century"), the GOP had hacked into Sony Pictures months in advanced.[22] The overall attack was described by Kevin Mandia (Sony's cybersecurity consultant) as being sophisticated, and "would have gotten past 90% of the net defenses that are out there in the private industry." It was speculated that this hack was also caused by a phishing attack, yet the exact cause has not yet been pinpointed.[23]

WHAT YOUR COMPANY CAN DO:

Again, ensure that your employees are vigilant in their attempts to spot false emails and other phishing attacks.

US OFFICE OF PERSONNEL MANAGEMENT

WHAT HAPPENED:

This hack has been described by observers as “the biggest government attack ever,” affecting 21.5 million people. Anyone who has ever worked for, or currently works for the United States government had their addresses, health information, financial history, and other private information swiped.

THE BLOODY AFTERMATH:

According to the New York Times, this breach has far-reaching consequences that span 15 years.24 Not only have former employees been affected, but about 1.8 million spouses and friends of these employees have also been exposed.

As James B. Comey Jr., the director of the FBI stated, “There is a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States government.” And that treasure trove was compromised.

LESSONS LEARNED:

The Inspector General (IG) characterized O.P.M defenses as having a “significant deficiency.” Among those deficiencies, the IT programs were handled by agency contractors. Users that accessed the O.P.M systems outside of the network didn’t go through a multi-factor authentication process.

The other troubling aspect of this breach is that there has been two decades of warnings that came from different auditors that poked holes in the gaping holes of the federal agency networks. But those warnings were ignored by agency officials.

WHAT YOUR COMPANY CAN DO:

Perform frequent audits on your systems to check for security vulnerabilities. Then, follow the directions of the auditors to fix said vulnerabilities. And, again, multi-factor authentication processes are a must.

LIVING SOCIAL

WHAT HAPPENED:

LivingSocial Inc. informed more than 50 million people that their personal information had been compromised. Emails, birthdates, and encrypted passwords were just the tip of the iceberg for lost data.

THE BLOODY AFTERMATH:

Although the hack didn't dip into the waters of financial and banking information, it left a profound impact. As Robert Hansen, Director of Product Management and Technical Evangelist at WhiteHat Security explained to CNET Magazine, "If there are approximately a billion people on the Internet, this hack single-handedly represents about half a percent of all Internet users."

As he further pointed out, the passwords that were breached can be reused over and over again by other parties.

LESSONS LEARNED:

LivingSocial CEO Tim O'Shaughnessy informed customers that the cyberattack stemmed from unauthorized access that reached internal SQL databases.

LivingSocial hasn't gone beyond those basic details to explain the origins of the attack. However, Chris Wysopal (an information security expert at Veracode) told CNET that, based on the type of data that was stolen, a certain type of web application was likely used to hit the SQL databases. Better testing could have been a possible way to get out in front of the breach.[25]

As was the case for Sony Pictures, reputational damage and the loss of trust are two sizeable fallouts that LivingSocial has naturally had to deal with. Kirk Nahra, a member of the advisory board for Bloomberg BNA's Privacy & Security Law Report, explained, "For the business, [the attack] was a tremendous confidence shaker, as it likely will lead to people becoming more reluctant to use this service."[26]

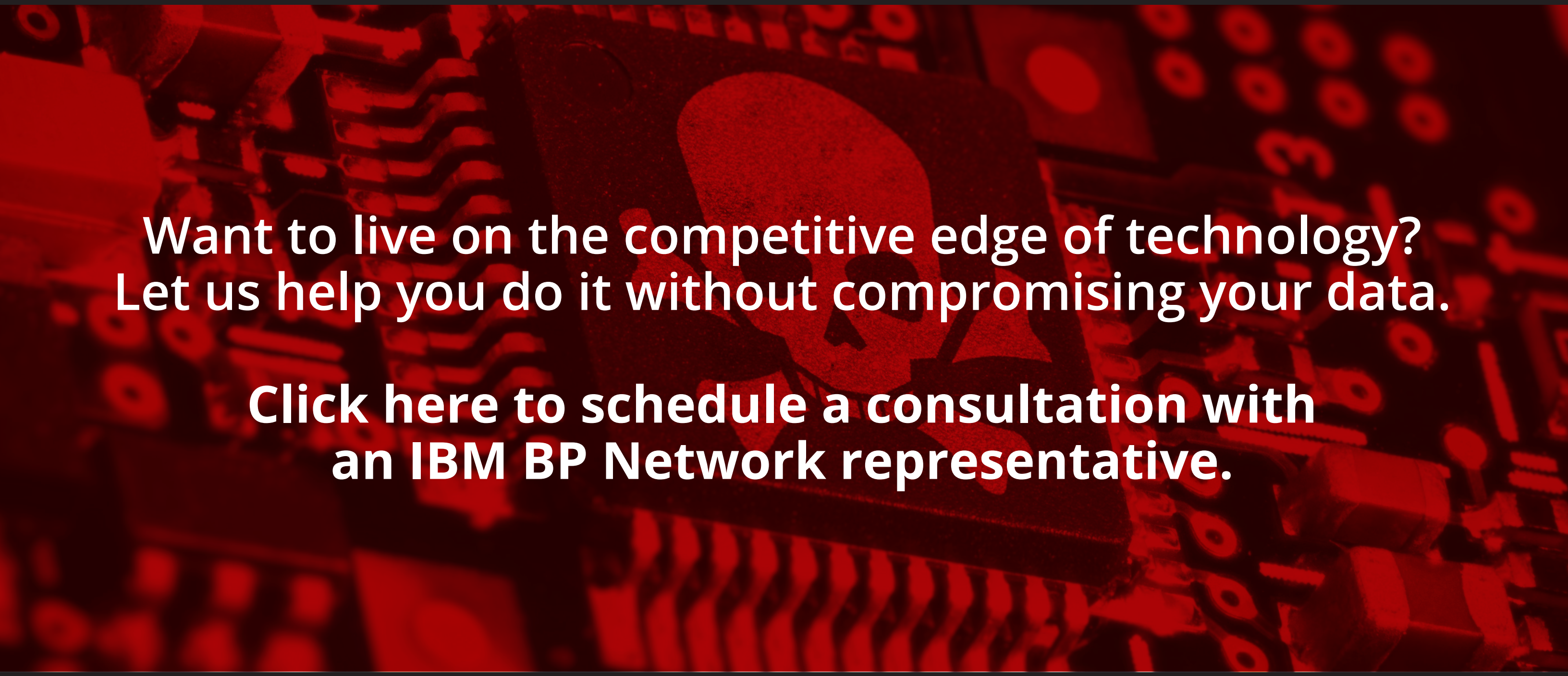
WHAT YOUR COMPANY CAN DO:

To ensure all systems are adequately protected from the latest threats, frequent security audits must be performed. Using third-party teams of ethical hackers is the best means of testing.

CONCLUSION

These are the hacks that will live in infamy.

Don’t let history repeat itself. Learn from the breaches of the past to make your security strategy that much stronger and fortified against the threats of tomorrow.



Want to live on the competitive edge of technology? Let us help you do it without compromising your data.

Click here to schedule a consultation with an IBM BP Network representative.

BP NETWORK

SOURCES :

1 Business Insider | http://www.businessinsider.com/how-to-access-the-deep-dark-web-2015-5

2 Forbes | http://www.forbes.com/sites/benkepes/2015/04/24/an-interesting-cyber-experiment-data-tracking-to-trace-the-dark-web/

3 WIRED | http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/

4 Krebs | http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/

5 Vormetric Insider Threat Report | http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf

6 Krebs on Security | http://krebsonsecurity.com/2014/11/home-depot-hackers-stole-53m-email-addreses/

7 https://www.us-cert.gov/ncas/alerts/TA15-119A

8 Washington Post | http://www.washingtonpost.com/business/economy/investigators-suspect-china-may-be-responsible-for-hack-of-anthem/2015/02/05/25fbb36e-ad56-11e4-9c91-e9d2f9fde644_story.html

9 Washington Post | https://www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/

10 The Wall Street Journal | http://www.wsj.com/articles/investigators-eye-china-in-anthem-hack-1423167560

11 Computer World | http://www.computerworld.com/article/2862578/twofactor-authentication-oversight-led-to-jpmorgan-breach-investigators-reportedly-found.html

12 NBC News | http://www.nbcnews.com/tech/security/target-reaches-settlement-visa-over-2013-data-breach-n412071

13 The Wall Street Journal | http://www.wsj.com/articles/target-nears-settlement-with-mastercard-over-data-

14 Krebs on Security | http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target/

15 PC World | http://www.pcworld.com/article/2457880/ebay-faces-class-action-suit-over-data-breach.html

16 The Washington Post | https://www.washingtonpost.com/news/the-switch/wp/2014/05/21/ebay-asks-145-million-users-to-change-passwords-after-data-breach/

17 SC Magazine | http://www.scmagazine.com/the-ebay-breach-explained/article/360998/2/

18 SC Magazine | http://www.scmagazine.com/the-ebay-breach-explained/article/360998/2/

19 The Seattle Times | http://www.seattletimes.com/seattle-news/premera-negligent-in-data-breach-5-lawsuits-claim/

20 The New York Times | http://www.nytimes.com/2015/03/18/business/premera-blue-cross-says-data-breach-exposed-medical-data.html?_r=0

21 http://www.npr.org/sections/alltechconsidered/2015/03/18/393868160/premera-blue-cross-cyberattack-exposed-millions-of-customer-records

22 Sony Pictures | http://fortune.com/sony-hack-part-1/

23 Wired | http://www.wired.com/2014/12/sony-hack-what-we-know/

24 The New York Times | http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=1

25 CNET | http://www.cnet.com/news/livingsocial-hacked-50-million-affected/

26 Bloomberg BNA | http://www.bna.com/livingsocial-reveals-cyberattack-n17179873787/