bitglass

KINGS OF THE MONSTER BREACHES

Regardless of the industries in which they operate, most organizations handle some type of sensitive data, like PII (personally identifiable information). If this information is not protected correctly, the resulting breaches can harm innocent people and, in many cases, cost massive amounts of money. To uncover trends and learn about the extent of damage that can be done, Bitglass researched the three largest breaches of publicly traded companies from each of the last three years. Key findings and analyses of these breaches can be found throughout the following pages. Additionally, large breaches of government and privately held organizations are described at the end of the report.

Key Findings

These leading breaches were caused by external cyberattacks that leveraged phishing, malware, technical vulnerabilities, and more.

The mean number of individuals affected by each breach was 257 million.

To date, these breaches have cost their companies an average of $347 million in legal fees, penalties, remediation costs, and other expenses.

On average, these enterprises suffered a 7.5% decrease in stock price after being breached, leading to a mean market cap loss of $5.4 billion per company. In comparison, the S&P 500 decreased an average of only 0.17% over the same time periods.

Even without Facebook, which was effectively an outlier that lost $43 billion in market cap, the average post-breach market cap loss was still $762 million.

While Equifax's stock price still has yet to recover, the others took an average of 46 days to return to their pre-breach levels.

MARRIOTT - 2018

On November 30, 2018, Marriott discovered that its Starwood Hotel branch had suffered a massive security breach. While the multinational hotel chain was uncertain about how the breach occurred, it did state that approximately 387 million guests had their names, dates of birth, gender, addresses, and passport numbers stolen. According to the report made to U.S regulators, unauthorized parties somehow gained access to reservations made between September 10, 2018 and, potentially, as far back as 2014.

- Marriott uncovered the breach while seeking GDPR compliance; the company is now being fined $912 million under the regulation
- Marriott experienced a 5.6% drop in share price following the breach
- There are multiple lawsuits pending, with firms seeking up to $12.5 billion in legal damages

Facebook - 2018

In September 2018, Facebook discovered a cyberattack on its internal network infrastructure. The attack compromised its users' names, genders, email addresses, location check-ins, and relationship statuses. The social media giant learned that the attack was made possible by three software coding issues. Two of the bugs were found in a tool developed to improve user privacy, while the third was associated with streamlined video uploading.

- Personal details of nearly 50 million users were compromised in Facebook's breach
- After the breach, Facebook's stock price decreased by 8%, yielding a $16 billion loss in market capitalization
- If found guilty of violating GDPR, the company could face fines as high as $1.6 billion

CHEGG - 2018

On September 19, 2018, Chegg discovered that it had been breached in April of that year. Hackers had managed to gain access to a database that contained millions of customers' PII, including names, email addresses, shipping addresses, usernames, and passwords. The encryption algorithm used to protect the data was apparently vulnerable to being cracked, demonstrating the need for a full-strength solution. The company took immediate action to notify its users and reset their passwords; however, after disclosing the breach, Chegg experienced its worst day of trading since going public in February 2016.

- 40 million users had their personal information exposed in Chegg's breach
- Chegg's stock plummeted 12% within a day of disclosing the hack
- The cost of the breach still has yet to be determined—the company is currently facing a class-action lawsuit

Equifax - 2017

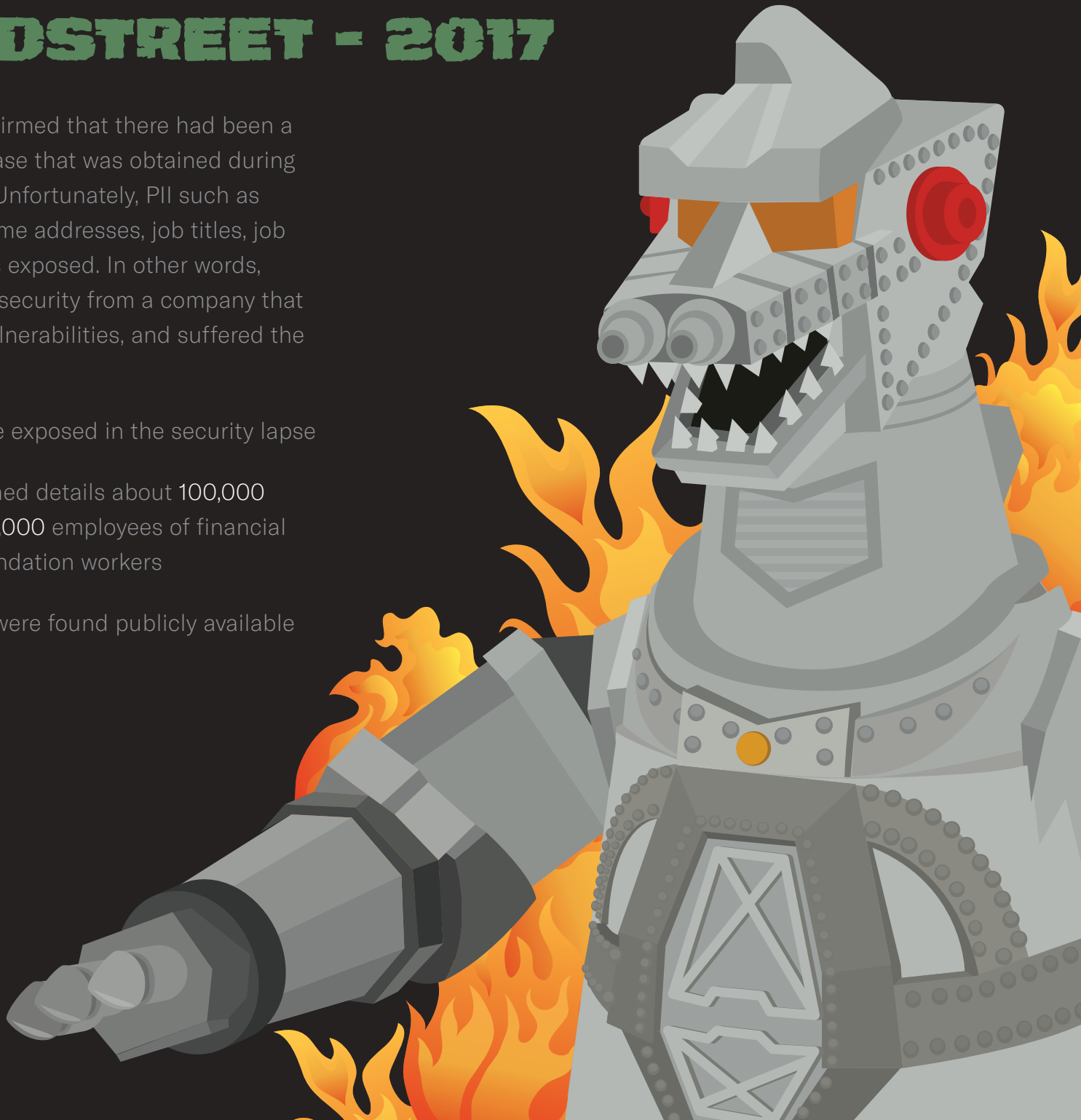
Equifax had one of the largest and most devastating data breaches of all time in September 2017. The event occurred because of a flaw in open-source software that was used by the credit reporting company. Through this vulnerability, hackers were able to access sensitive data such as Social Security numbers, credit card numbers, full names, dates of birth, and home addresses. It took roughly two months for the breach to be discovered. The company's CSO, Susan Mauldin, and CIO, David Webb, retired immediately after the security lapse had been announced.

- Shares of Equifax dropped nearly 14% the day after the announcement, and 31% within two weeks
- Over 143 million people had their personal information impacted by the event
- Equifax faced $439 million in legal, remediation, insurance, and investigation costs

Dun & Bradstreet - 2017

In March 2017, Dun & Bradstreet confirmed that there had been a breach of information within a database that was obtained during the acquisition of another company. Unfortunately, PII such as names, personal email addresses, home addresses, job titles, job functions, work emails, and more was exposed. In other words, Dun & Bradstreet inherited improper security from a company that it purchased, failed to address the vulnerabilities, and suffered the consequences.

- Over 33 million unique records were exposed in the security lapse
- The compromised database contained details about 100,000 Department of Defense workers, 70,000 employees of financial institutions, and 35,000 Kaiser Foundation workers
- 14% of the compromised accounts were found publicly available online following the breach



Sonic Drive-In - 2017

In September 2017, Sonic Drive-In discovered that it had fallen victim to a breach when its credit card processor identified unusual activity. While Sonic hasn't officially disclosed how the breach occurred, it was likely caused by malware installed on one or more point-of-sale terminals. Regardless of the cause, the goal of the attack was to compromise customer credit card information. Of the 3,600 locations in the US, 325 were affected by the six-month malware attack.

- 5 million credit cards from this attack were found for sale online
- Sonic paid $4.3 million in legal damages
- Following the breach, the company's share price dropped by 3.5% in less than one week

YAHOO! - 2016

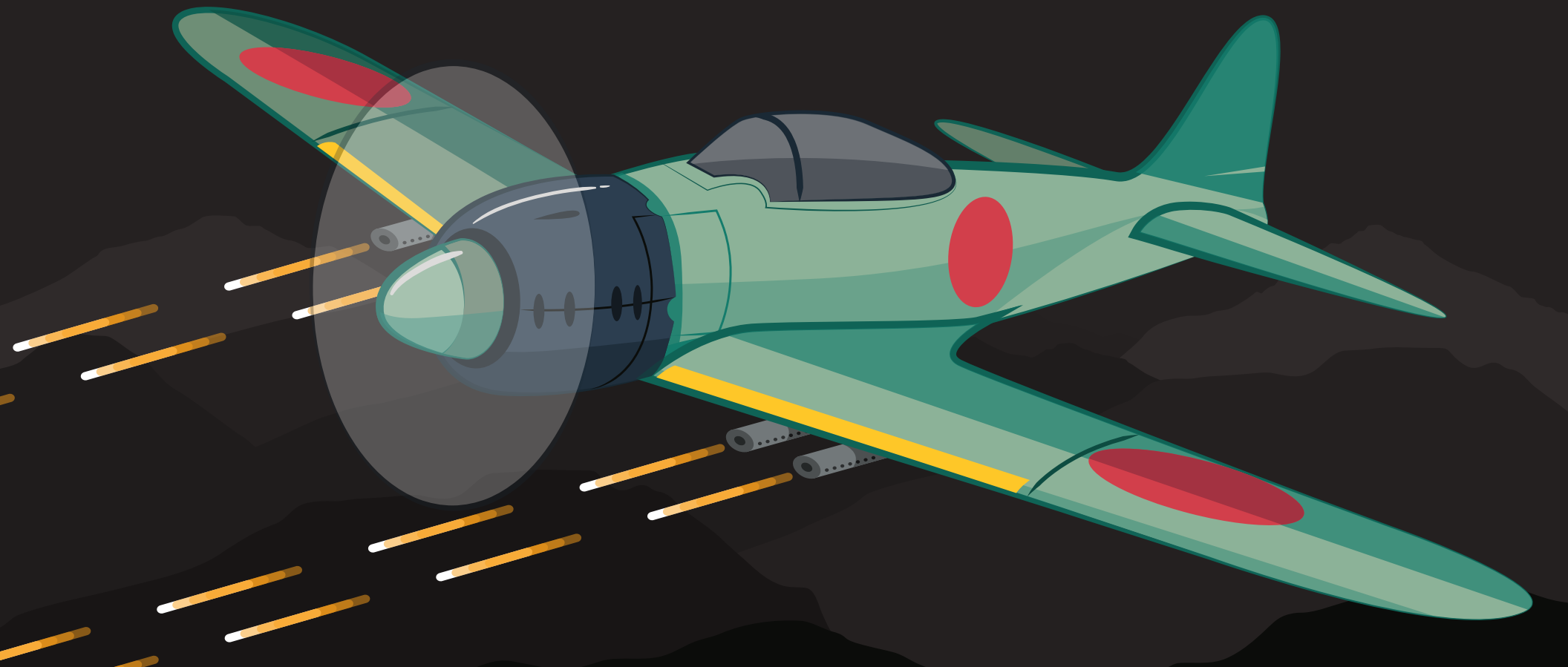
In 2016, Yahoo! announced that it had faced two separate breaches—one in September, which compromised over 500 million account holders, and another in December, which affected over 1 billion. Compromised information included PII that was initially collected in 2014 and was used through December of 2016. In the state-sponsored phishing attacks, hackers stole data such as users' names, email addresses, phone numbers, birthdays, passwords, as well as their answers to security questions.

- Yahoo! spent over $95 million on remediation and legal fees
- The company was fined an additional $35 million for its failure to disclose the hacks to investors
- Because of the breaches, Verizon purchased Yahoo! for $350 million less than it originally offered

LinkedIn - 2016

In late 2016, LinkedIn learned that millions of its users' login credentials had been stolen. Consequently, the company promptly notified account holders that they needed to change their passwords. Hackers had managed to circumvent the inadequate encryption that LinkedIn had in place and gained unauthorized access to the company's store of user credentials. Initially, LinkedIn believed that 6.5 million accounts were affected; however, the company later determined that tens of millions more were compromised.

- 167 million user accounts were compromised in the breach
- Hackers used the stolen passwords to sign in to 90% of their victims' accounts within 72 hours.
- News of the breach led to a 4% drop in share price within a week



Verizon Enterprise - 2016

On March 24, 2016, Verizon Enterprise, a division of Verizon focused on corporate clients, discovered that the PII of 1.5 million customers was compromised. The corporation confirmed the breach when it found the aforementioned personal details for sale on an underground cybercrime forum. Unfortunately, as 97% of Fortune 500 companies use Verizon Enterprise, the employees of these and other organizations are now at greater risk of falling prey to targeted spear phishing attacks that leverage the appropriated PII.

- The stolen data was being sold for $100,000; subsets could be purchased for $10,000 a piece
- In addition to selling the stolen information, hackers offered details about the vulnerabilities that they exploited in the breach
- The breach occurred because of a security flaw on Verizon's website that gave hackers access to an unsecured MongoDB server

Private Companies & Government Agencies

Exactis

Exactis, a firm that collects consumer data for targeted ads, experienced an immense breach in June 2018. Publicly accessible databases exposed 340 million business and consumer accounts. 400 data points were compromised per account, including home address, email address, age, number of children, religious affiliations, and even household pets. While no financial information is reported to have been leaked, the compromised data can still enable impersonation, profiling, and targeted spear phishing.

- The compromised database was reported to contain information about almost every US citizen
- 230 million consumer accounts and 110 million business accounts were exposed in the breach

Uber

In late 2016, hackers gained access to the personal data of millions of Uber users and drivers by stealing credentials to the company's AWS instance. 57 million individuals had their PII appropriated—this included their phone numbers, email addresses, and names. Additionally, hundreds of thousands of drivers had their Driver License numbers stolen. Ultimately, Uber paid $148 million in settlement.

- Uber paid the attackers $100,000 and made them sign a non-disclosure agreement in hopes of hiding the breach
- Chief Security Officer John Sullivan and Chief Executive Officer Travis Kalanick were fired once the events came to light

The National Security Agency (NSA)

In August of 2016, a cybercriminal group known as Shadow Brokers published samples of code that demonstrated that they had extensive knowledge of the NSA's IT systems and tools. The group was supposedly using stolen NSA information to enable its hacking. The fact that the NSA was vulnerable to hackers evinces the fact that even the most trusted organizations are not invincible.

- Shadow Brokers gained access to tools that the NSA was using to hack other nation states
- Following the breach, compromised NSA data was found for sale for $1 million

Wrap-Up

The breaches that struck the organizations in this report should serve as a warning to enterprises around the globe. Breaches can be the result of misconfigurations, malware, phishing, and much more; additionally, they can do massive damage to companies and their various stakeholders. As such, organizations must adopt a proactive approach to cybersecurity before they are faced with any of the scenarios detailed on the previous pages. Fortunately, there are security solutions capable of securing data wherever it goes.

bitglass

Phone: (408) 337-0190
Email: info@bitglass.com

www.bitglass.com

About Bitglass

Bitglass, the Next-Gen CASB company, is based in Silicon Valley with offices worldwide. The company's cloud security solutions deliver zero-day, agentless, data and threat protection for any app, any device, anywhere. Bitglass is backed by Tier 1 investors and was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution.