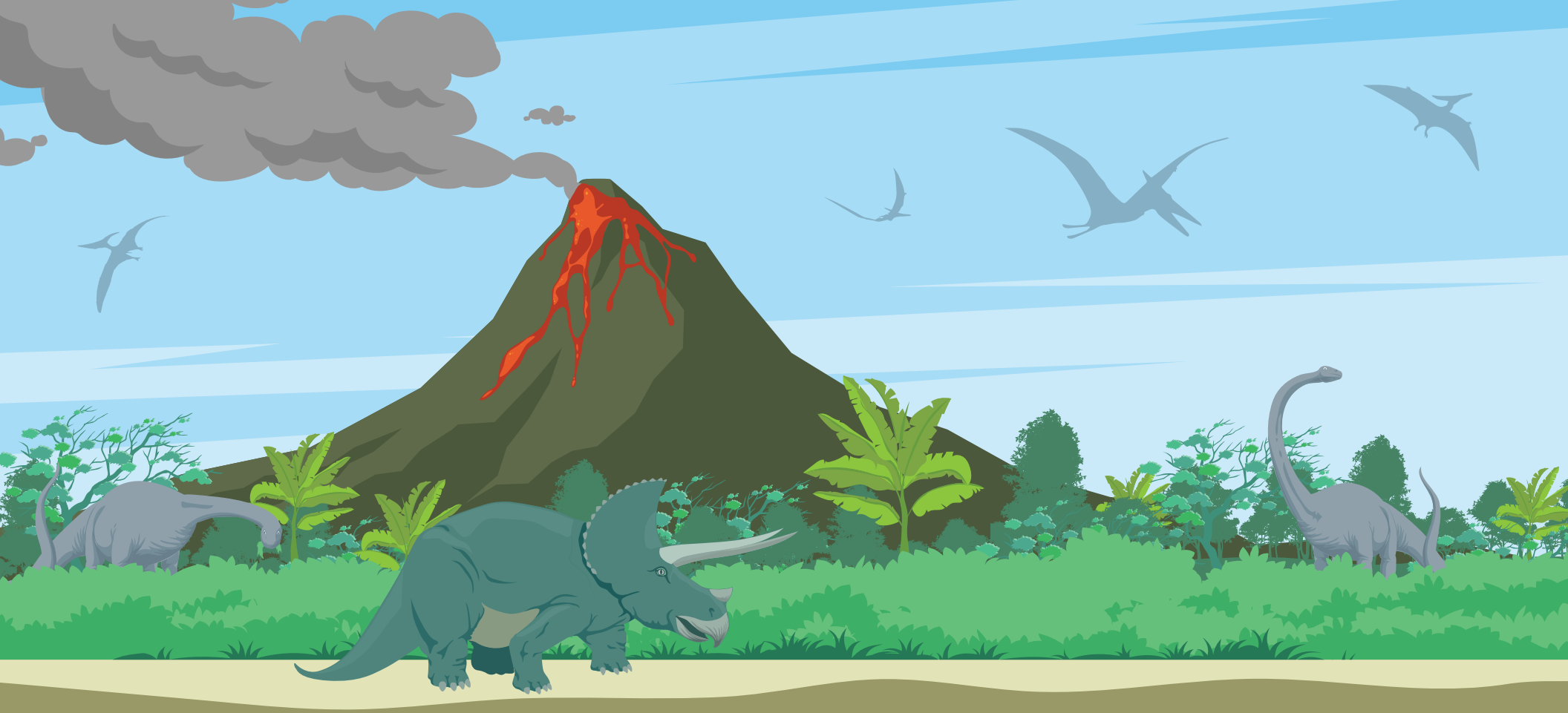
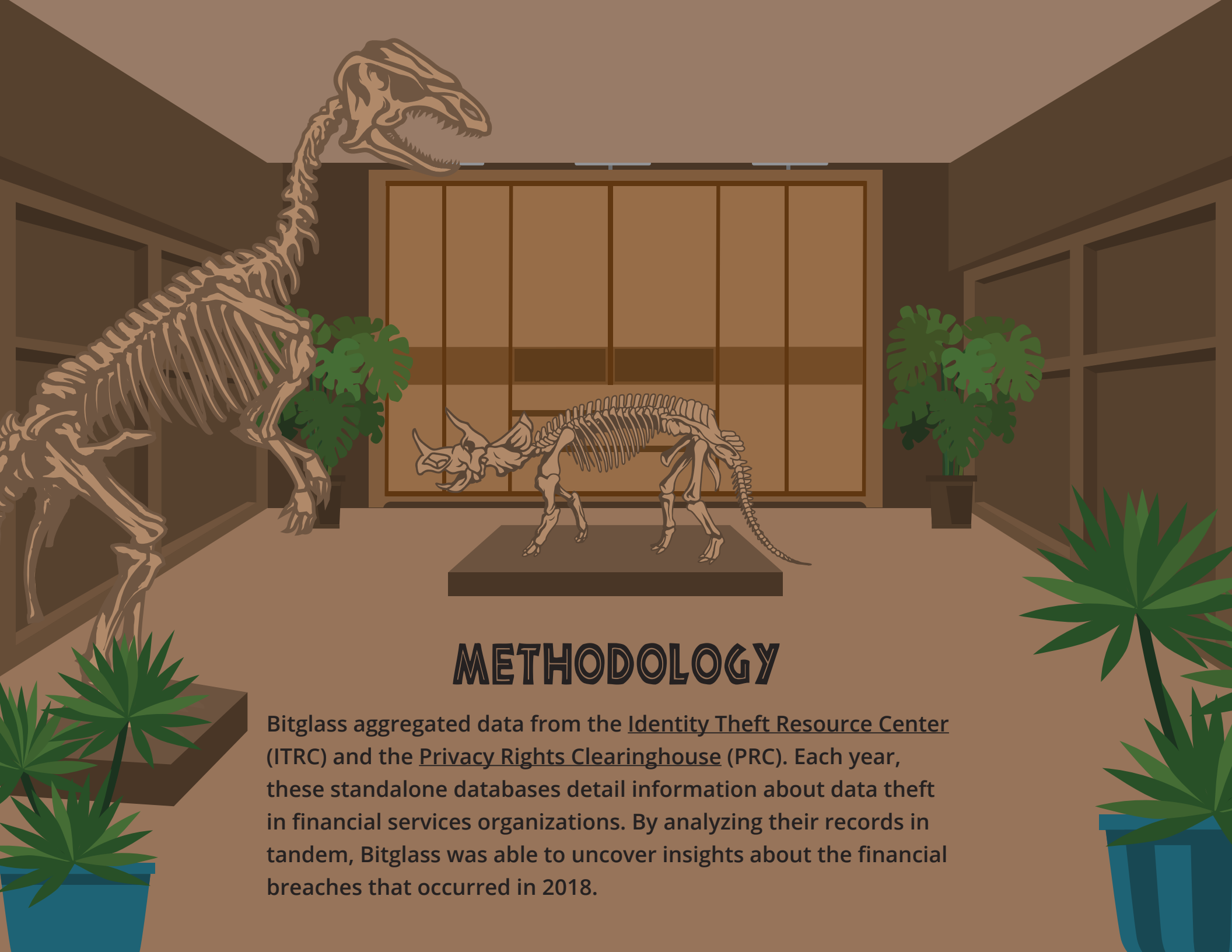
bitglass

FINANCIAL BREACH REPORT 2018



Financial services firms must be highly vigilant when it comes to cybersecurity. They regularly handle sensitive, regulated data like customers' home addresses, bank statements, Social Security numbers, and more. Naturally, this type of information is the lifeblood of any organization and constitutes an attractive target for criminals. With this in mind, Bitglass set out to uncover the state of security in financial services in 2018.



METHODOLOGY

Bitglass aggregated data from the Identity Theft Resource Center (ITRC) and the Privacy Rights Clearinghouse (PRC). Each year, these standalone databases detail information about data theft in financial services organizations. By analyzing their records in tandem, Bitglass was able to uncover insights about the financial breaches that occurred in 2018.

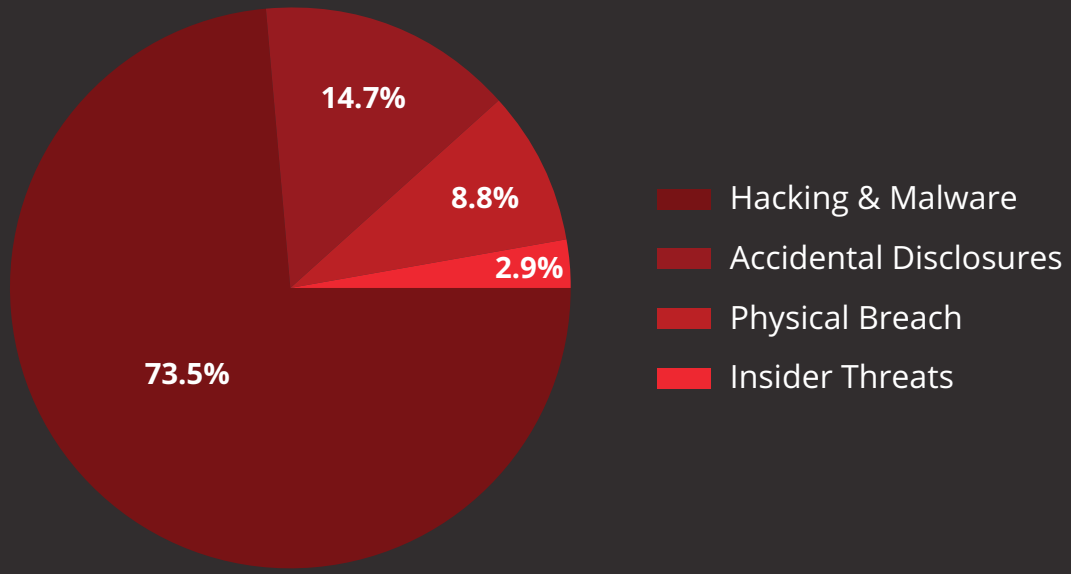
EVOLUTION IN ACTION

For financial services firms, 2018 has been far more dangerous than 2016. From January to August of this year, there were nearly three times as many breaches as there were over the same period in 2016. Unsurprisingly, hacking and malware were largely responsible for this rise in breaches. As malware continues to spread and evolve, it should be a top concern in financial services.

The 103 breaches recorded in 2018 have nearly tripled the 37 recorded over the same time frame in 2016.

Hacking and malware were responsible for nearly three quarters of all financial services breaches in 2018, up from an average of 20% over the last several years.

Causes of Breaches in 2018



THE NEW T-REX

Malware has quickly emerged as the king of threats. In a recent Bitglass study, Malware, P.I., nearly half of all organizations were found to be infected. Additionally, incredibly few anti-malware tools proved capable of detecting ShurL0ckr, which was a new, zero-day piece of malware. Clearly, the need for advanced, behavior-based threat detection is at an all-time high.

Google Drive, Microsoft SharePoint, and 93% of antivirus engines were unable to detect the zero-day ransomware ShurL0ckr.

44% of organizations have malware in at least one of their cloud apps.

So far in 2018, ransomware like WannaCry has continued to spread, and Emotet has emerged as a leading, modular banking trojan. Cloud cryptojacking is also on the rise. Security experts are particularly concerned by the evolution of context-aware threats like the Rakhni Trojan, as well as the growth of ransomware-as-a-service, wherein hackers offer ransomware platforms that inexperienced cybercriminals can use to hold data hostage.

DINO FOOD

A number of reputable financial services firms have already been breached in 2018. The fact that these industry leaders were unable to protect their data demonstrates how challenging it can be to ensure cybersecurity. Clearly, no organizations can assume that they are invulnerable—particularly as data moves to more applications and devices than ever before.

dun & bradstreet

JPMorganChase

RBC Royal Bank

SallieMae

Goldman Sachs

Citizens Financial Group, Inc.

Fidelity INVESTMENTS

PennMutual

Golden1 Credit Union

intuit

JURASSIC-SIZED BREACHES

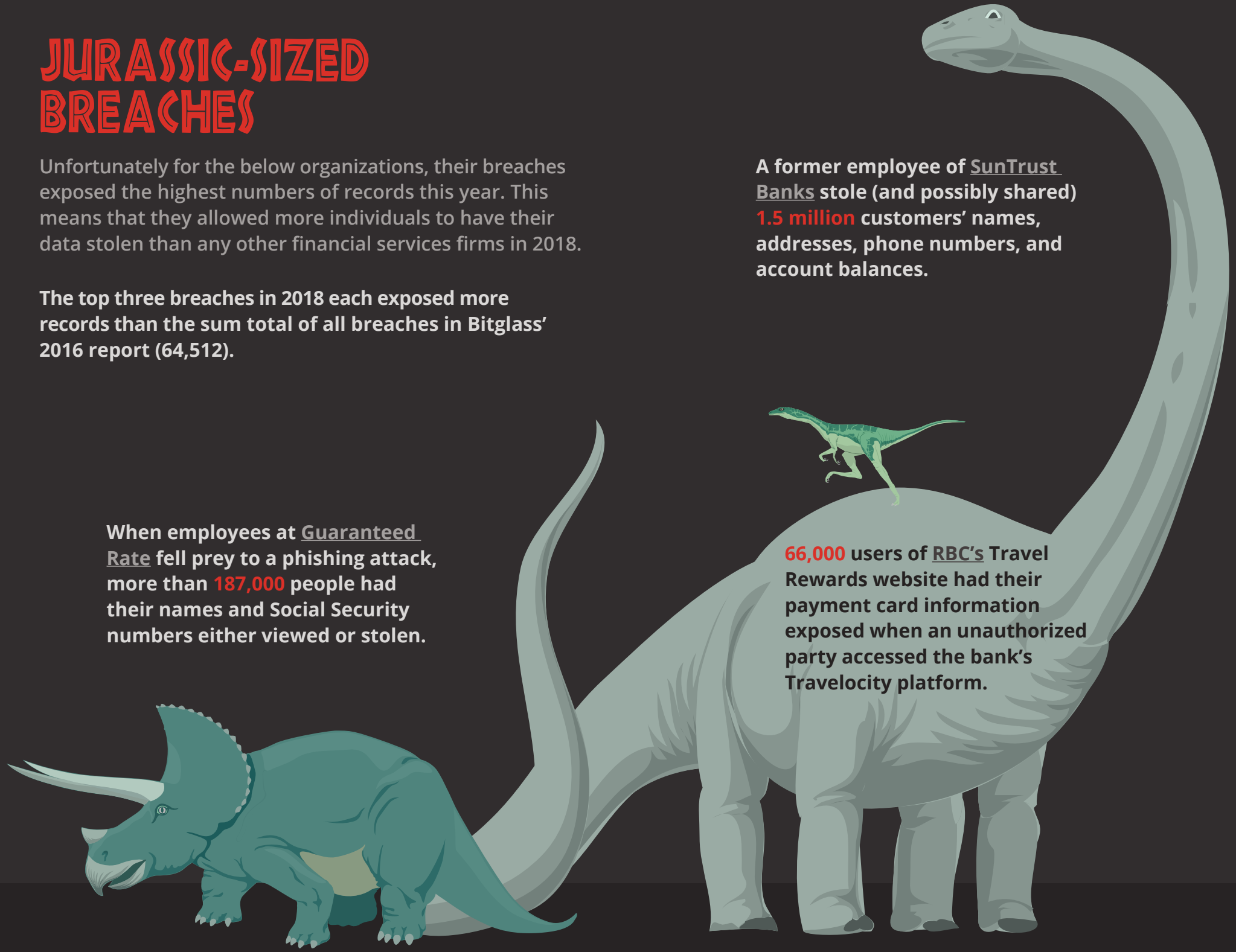
Unfortunately for the below organizations, their breaches exposed the highest numbers of records this year. This means that they allowed more individuals to have their data stolen than any other financial services firms in 2018.

The top three breaches in 2018 each exposed more records than the sum total of all breaches in Bitglass' 2016 report (64,512).

A former employee of SunTrust Banks stole (and possibly shared) 1.5 million customers' names, addresses, phone numbers, and account balances.

When employees at Guaranteed Rate fell prey to a phishing attack, more than 187,000 people had their names and Social Security numbers either viewed or stolen.

66,000 users of RBC's Travel Rewards website had their payment card information exposed when an unauthorized party accessed the bank's Travelocity platform.



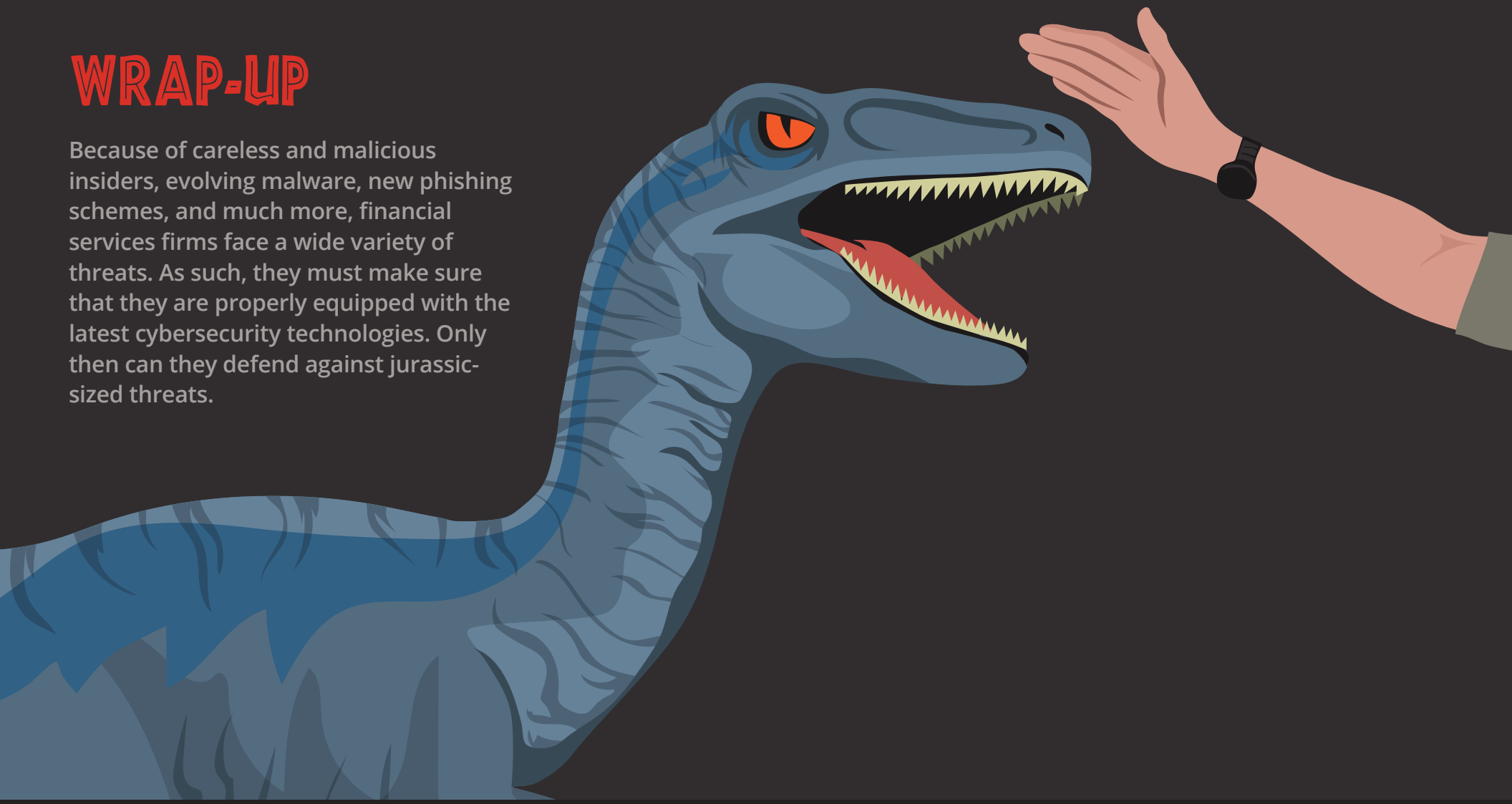
LOCKING DOWN THE PARK

Regulations like the Gramm-Leach-Bliley Act (GLBA), the Payment Card Industry Data Security Standard (PCI DSS), and the Sarbanes-Oxley Act (SOX) are designed to ensure that organizations are protecting their customers' financial information. They contain various requirements related to securing data access, responding to cyberattacks, and much more. For those who fail to comply, fines can amount to $100,000 per infraction under GLBA, $500,000 per infraction under PCI DSS, and more than $5 million under SOX. In addition to these penalties, breaches can harm organizations' reputations and, consequently, revenues.

Financial services firms that want to succeed simply cannot afford to maintain a lax security posture.

WRAP-UP

Because of careless and malicious insiders, evolving malware, new phishing schemes, and much more, financial services firms face a wide variety of threats. As such, they must make sure that they are properly equipped with the latest cybersecurity technologies. Only then can they defend against jurassic-sized threats.



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.