FINANCIAL SERVICES
BREACH REPORT

The financial sector struggles with data leakage in part because many such organizations rely on dinosaurs - security solutions that struggle to protect data outside the corporate network. These orgs also handle large quantities of high-value data—everything from customer names and addresses to social security numbers, bank balances, detailed transaction history, and more. Naturally, security is a top priority for all enterprises in the sector, however cyber-attacks, lost devices, and unintended disclosures continue to plague the industry.

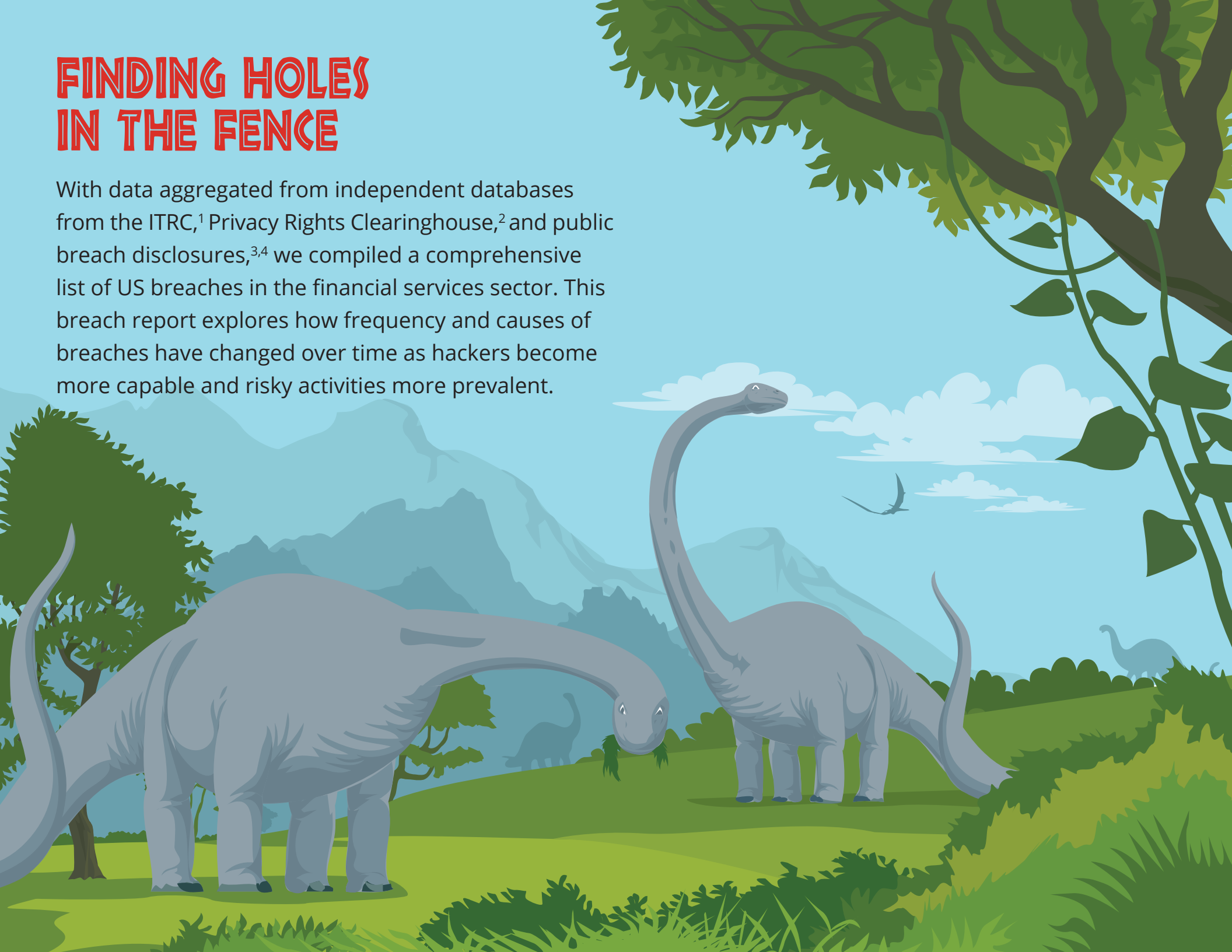
At Bitglass, we were curious to learn more about the state of financial services security as banks, accounting firms, and credit institutions migrate to the cloud.

- *Have breaches declined since the massive Heartland Payments leak in 2008?*
- *What proportion of breaches are the result of hacking?*
- *How common are recurring breaches?*

We answer those questions and more in our Financial Services Breach Report.

FINDING HOLES IN THE FENCE

With data aggregated from independent databases from the ITRC,[1] Privacy Rights Clearinghouse,[2] and public breach disclosures,[3,4] we compiled a comprehensive list of US breaches in the financial services sector. This breach report explores how frequency and causes of breaches have changed over time as hackers become more capable and risky activities more prevalent.

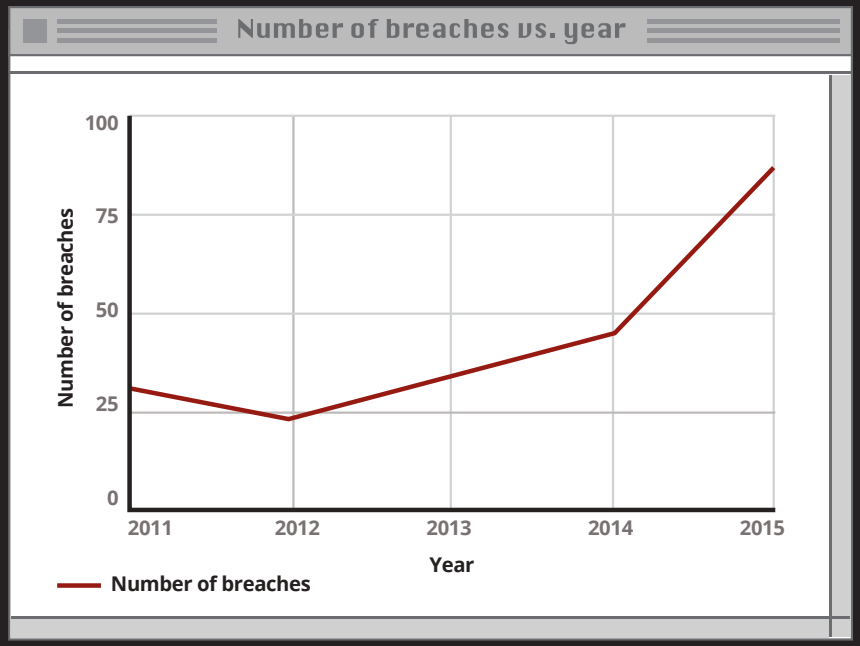


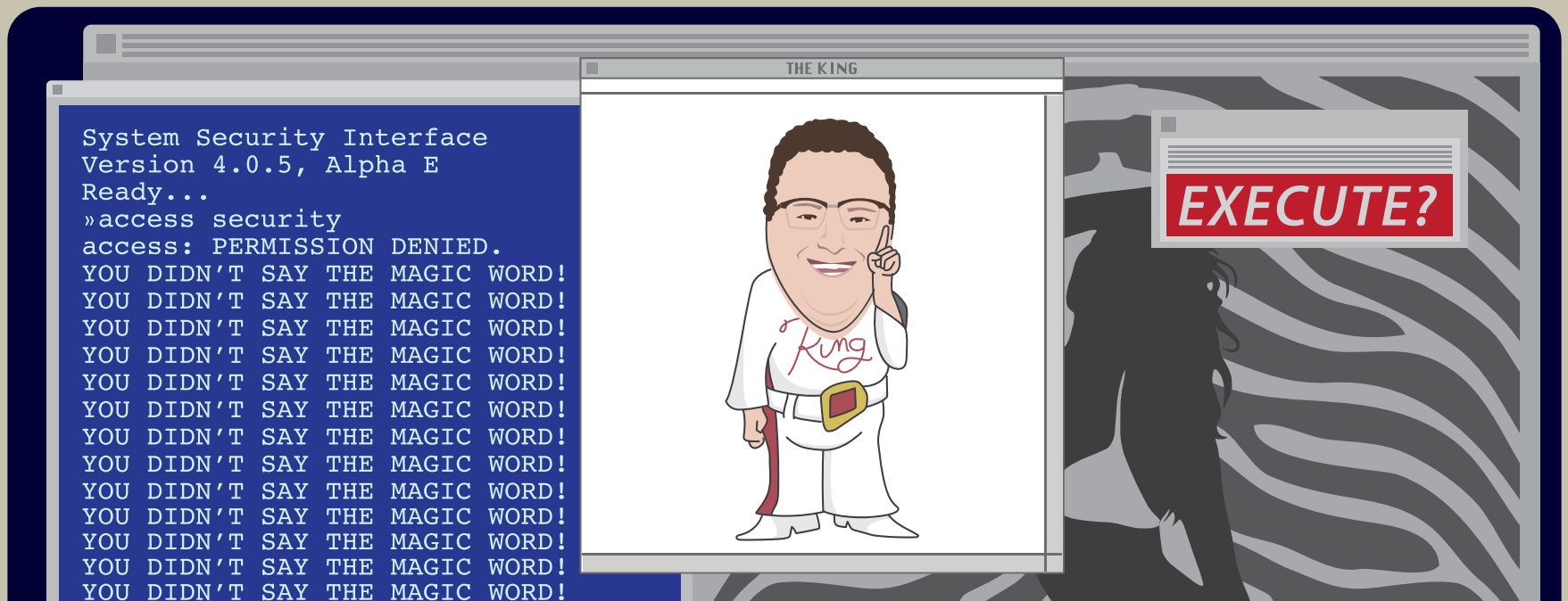
FINDINGS

- One in four breaches in the financial services sector over the last several years were due to lost or stolen devices, one in five were the result of hacking. 14 percent of leaks can be attributed to unintended disclosures and 13 percent to malicious insiders.)
- Five of the nation's 20 largest banks have already suffered data breaches in the first half of 2016.
- In 2015, at least 87 breaches were reported in the financial services sector, up from 45 in 2014. Already in the first half of 2016, 37 breaches were disclosed.
- Over 60 organizations suffered recurring breaches in the last decade, including most major banks.
- JP Morgan Chase, the nation's largest bank, has suffered several recurring breaches since 2007. The largest breach event, the result of a cyber-attack, was widely publicized in 2014 and affected an estimated 76 million US households. Other breaches at JPMorgan were due to lost devices, unintended disclosures, and payment card fraud.
- Breaches on the part of payment processors continue to lead all other types of organizations in the sector, with Heartland ('09, 130M), CardSystems ('05, 40M), iBill ('06, 17M), Global Payments ('12, 7M), and CheckFree Corp ('09, 5M) among the largest breaches in the last decade.
- Of the three major credit bureaus, the 2015 Experian leak was the largest, affecting 15 million individuals. Equifax has also disclosed several recent breaches, including unauthorized accesses earlier this year that affected hundreds of thousands.

DATA BREACHES ARE AT AN ALL-TIME HIGH

The number of breaches in financial services is accelerating year after year. In 2015, 87 organizations reported a breach, up from 45 in 2014. Already in the first half of 2016, 37 firms in the sector experienced a breach—on track to match or surpass the number of breaches in previous years. These growing counts likely underestimate the number of breaches in the sector as many smaller orgs may have failed to disclose minor leaks. The increase in frequency of breaches suggests data security is not a solved problem, but a growing problem for the sector.





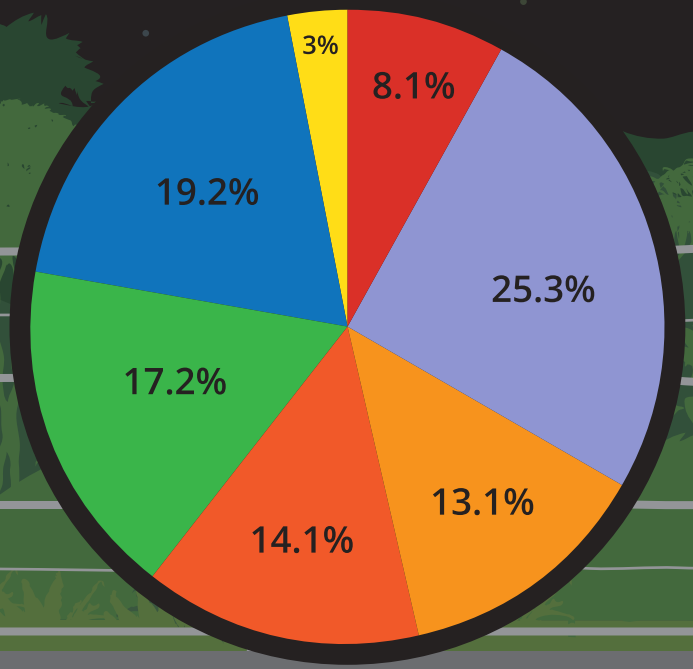
CYBER-ATTACKS ARE ONLY PART OF THE PROBLEM

The highly publicized breaches at JPMorgan Chase in 2014, Citibank in 2011, and Heartland in 2009, were all the result of hacking. A disproportionate number of individuals are affected by these hacking-related breaches as compared to other causes. A closer look at each disclosure reveals that lost and stolen devices are in fact the most frequent cause of data leakage, accounting for one in four breaches over the last decade. Hacking follows at one in five.

As damaging as phishing attacks and lost mobile phones can be, insider threats and unintended disclosures should be of equal concern to enterprises that handle sensitive financial information. Accounting for 14 percent of breaches, unintended disclosures are often the result of an accidental external share or email, made easier by cloud apps. For organizations without visibility into user activity, it is difficult, if not impossible, to determine which files contain PII or PCI and to prevent these unintended disclosures. Insider threats have comprised just over 13 percent of breaches in the last decade, a threat that can be mitigated where organizations have the ability to analyze user behavior and quickly identify any anomalies.

BREACH TYPES SINCE 2006

- Payment Card Fraud
- Lost Paper Records
- Lost or Stolen Device
- Insider Breach
- Unintended Disclosure
- Unknown
- Hacking

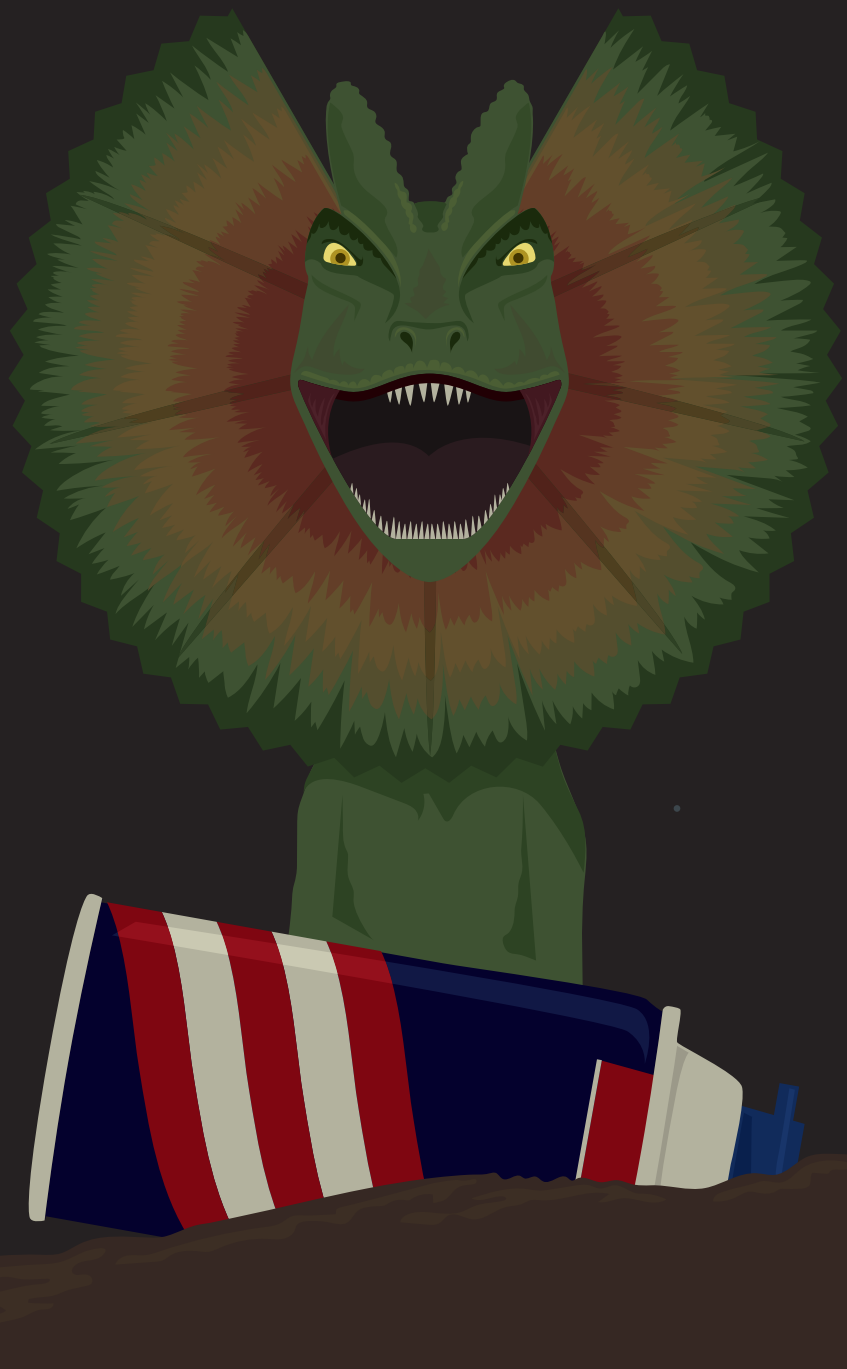


DANGER: EVEN A SMALL BREACH CAN COST MILLIONS

A Ponemon Institute report[5] earlier this year estimated that the average cost per lost or stolen record in the US is $221. Financial services organizations face a much higher average cost per lost record—$264. With millions of customers, large banks are subject to material penalties as a result of a breach. For smaller regional banks with hundreds of thousands of customer records - the costs can be devastating.

Among the costs are penalties levied once organizations are found in violation of government mandates or industry-imposed self-regulation. Many of these mandates require technical safeguards, but oftentimes, organizations leave a gap in their security—be that uncontrolled access to a cloud app or inadequate visibility.

GLBA is one major regulatory concern for financial services organizations—mandating strong passwords, encryption for data in transit, and the ability to detect and respond to attacks. SOX requires security controls over sensitive financial data, and PCI applies to financial services orgs that handle payment cards. What these regulatory mandates share are incredibly high penalties. PCI-DSS penalties can reach $500K per incident, GLBA up to $100K per incident, and SOX up to $5M per incident. All data handled by financial firms can be protected where IT has proper access controls, strong cloud encryption, and a real-time inline solution in place.



A PROACTIVE APPROACH TO PARK SECURITY

As cloud apps become increasingly pervasive, more secure, and more capable than premises-based apps, financial services orgs are migrating in droves. 37.5% of such firms had some cloud app deployed in 2015.[6] The cloud offers improved infrastructure and application security with teams dedicated to staying several steps ahead of hackers.

Data security remains the responsibility of the enterprise. For financial services orgs, this means protecting data-at-rest in the cloud with robust encryption, deep visibility, and data leakage prevention policies to watermark or redact sensitive data at download. Cloud Access Security Brokers (CASBs) have become the go-to solution for enterprises that need a comprehensive security solution to protect data in the cloud and on any device.

HIGH VALUE, HIGH RISK

Financial services firms are prime targets for hackers because of the volume of sensitive data they store and use. From home addresses to social security numbers, these banks, credit processors, and accounting firms store incredibly detailed financial information on all Americans, and a single breach can put millions at risk. Many of these breaches, far more common and costly than enterprises may realize, can easily be prevented with the appropriate controls in place.

As financial services firms migrate to the cloud, it is important for IT departments to consider the realities of data access and device usage today—to choose a security solution that mitigates risk of data leakage, that is trusted by peer organizations, and that protects data from cloud to device for compliance with regulatory mandates.

ABOUT BITGLASS

bitglass

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

www.bitglass.com

The Bitglass Cloud Access Security Broker (CASB) solution provides end-to-end data protection from the cloud to the device. It deploys in minutes and works with any cloud app on any device. Bitglass enables enterprises to understand and control usage of cloud apps like Office 365 and Salesforce, and internal apps like Exchange and Sharepoint. Cloud data at rest is protected with encryption and suspicious activity detection. IT security teams can enforce consistent access, sharing, and data leakage prevention policies across multiple cloud services, and protect data on mobile devices—without MDM.

SOURCES

1 http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf
2 https://www.privacyrights.org/
3 https://www.oag.state.md.us/idtheft/breachNotices2015.htm
4 http://www.in.gov/attorneygeneral/files/2015_04_01_ITU_Breach(3).pdf
5 http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094USEN
6 http://www.bitglass.com/infographics/financial-services-cloud-adoption