# Banking Industry Cyber Threats

WHITE PAPER

## INTRODUCTION

This white paper covers threats facing the banking industry outside the traditional firewall perimeter, stemming from both lack of control over assets and an ever-growing set of website and mobile vulnerabilities.

The banking industry continues to be a focus of an increasing number of security attacks, which has resulted in significant financial loss and data exfiltration for many institutions. The most prominent information security strategy in the industry remains a defense in depth approach tied to the belief that the perimeter to be defended is the firm's firewall and internal network. While this strategy might stave off some attacks, it does little to protect the customers, brand equity or reputation of banks.

Defense in depth, derived from ancient military strategy and also known as the Castle Approach, involves successive, independent layers of security—like the moats and walls of an actual castle—to protect a set of assets. Ideally, this approach helps to both detect and delay or prevent attacks, buying time for IT organizations to respond to threats. While this strategy—mirroring the vaults and alarms in brick and mortar bank branches—seems sound, three things must be true for it to be successful:

1. **The assets you need to protect are inside the perimeter.**
2. **The attackers are outside the perimeter.**
3. **The perimeter's defenses are adequate to stop or impede the attackers.**

Current banking industry security practices often fail on the first two necessities, making the third difficult or impossible. These failures largely come from incorrectly defining the perimeter to be secured, leaving many assets outside the castle and vulnerable to attacks.

Most banks view their potential attack surfaces as relatively small—contained within their firewalls and internal networks. However, the attack surface is far more expansive—often by several orders of magnitude—and many assets lie beyond the perimeter, unbeknownst to the banks. With both consumer and enterprise banking transactions becoming increasingly ubiquitous worldwide via websites and mobile apps, the perimeter you need to defend does not end at the firewall—it is the entire Internet, every PC and every mobile device. The list of assets necessary to defend has expanded to include the bank's customers, websites and apps, in addition to its internal monetary assets and employees.

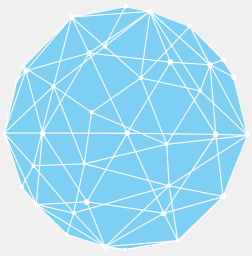
For a quantitative assessment of the threats facing banks, RiskIQ performed a detailed survey in April 2015 of the websites, web assets and mobile apps associated with each of the top 35 banks and financial service firms, checking for potential security issues and weaknesses. The results from the survey show that even rigorous internal security practices protect against only a small part of the potential threats facing your brand and customers.

## DIGITAL FOOTPRINT

RiskIQ is the only security company that scans the entire Internet millions of times per hour, collecting telemetric data to produce a dynamic index of web attack surfaces—illuminating websites, mobile apps, URLs, web page content, ASNs, IPs and nameservers. Using RiskIQ Enterprise Digital Footprint on the 35 leading financial service firms in North America, we uncovered a massive array of digital assets appearing online tying back to those organizations.

35

major financial services firms or banks



260k

web assets

1,777

mobile apps

## WHAT'S AT RISK?

The traditional motives of criminals attacking banks was to remove the bank's assets and to empty accounts or divert payments. While still a risk, account takeover is no longer the only goal for attackers. Online banking also provides significant non-cash assets that can be exploited or stolen by increasingly sophisticated attackers. These at-risk assets can be divided into two key categories:

1. **Tangible:** The personally identifiable information (PII) of banking customers needed to collect and retain for internal operations and regulatory reporting
2. **Intangible:** The trust and confidence placed in banks and their brands by consumers

Security breaches, whether they involve direct theft of data or just leverage a bank's brand to commit fraud, can have a significant impact on profitability and resources. The potential losses are especially high in an industry like banking where consumer confidence and brand equity are critical factors in customer base growth and retention.

Examples of damages from the security threats uncovered in the RiskIQ study include:

- Direct losses from theft of funds—this is often the type of loss that gets the largest portion of media attention, though it may be a small fraction of the total damages
- Denial of service attacks making all or part of a bank's web or mobile presence inaccessible
- Costs from customer notification and remediation—like credit report and identity recovery—plus public relation expenses from managing media inquiries
- Damage to the bank's brand equity and reputation, creating abnormal customer churn and making acquisition of new customers more costly
- Violations of data privacy regulations, which can result in increased regulatory scrutiny at both the federal and state levels and impact profits, IT costs and business agility
- Lost opportunity costs from time spent addressing or remediating security threats

In addition to these impacts on banks, the organization within the bank entrusted with the information security infrastructure is also negatively impacted. Losses perceived to be due to or aggravated by negligence can result in derailed careers or resignations for both security professionals and executives. While some banks will have cyber insurance policies to recover certain costs from an attack, serious exploits that impact customers will consume significant resources beyond many coverage limits.

The potential losses don't stop just at the bank's income statements. For example, when a consumer's financial information is stolen, the bank often needs to pay for new debit, credit and ATM cards to be issued at an estimated cost of $10 per card.[1] These costs flow back to the card issuers and payment processors who may try to recover them from the breached bank.

## RISKIQ'S SURVEY OF 35 TOP BANKS AND FINANCIAL SERVICES FIRMS

To understand the magnitude of potential threats outside the firewall, RiskIQ has performed a detailed, quantitative assessment of potential vulnerabilities facing the banking industry. The survey was conducted in April 2015 and included a complete scan of the web presence and mobile apps associated with 35 top banks, both regional banks with brick and mortar branch locations and online-only banks/brokerages.

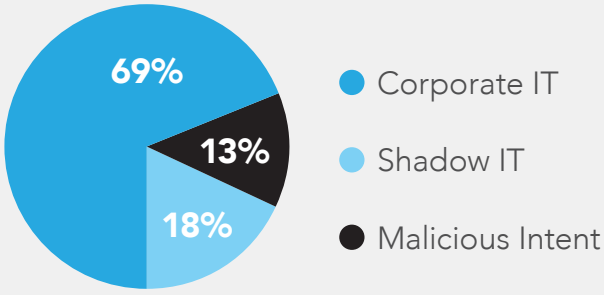
At a high level, these threats can be segmented by:

1. **The delivery system used to reach consumers:** e.g. redirecting or pharming websites and web assets, brand spoofing via unauthorized apps and assets, phishing emails, etc.
2. **The source of the vulnerability:** e.g. software and communications security flaws, scripting languages, third-party components and libraries, uncontrolled asset hosting leading to injection of rogue or compromised assets, software bugs, etc.

The survey involved running RiskIQ's proprietary Enterprise Digital Footprint scanning tool against websites and mobile apps created by bank IT groups and by both authorized and unauthorized third parties. Websites in the survey's scope included main websites, secondary websites, co-branded affiliate sites, marketing landing pages, co-branded partner sites, third-party created sites, mobile apps, social media profiles and more.

In addition, RiskIQ looked at third-party components and external hosting used for the banks' websites and web assets, as these are often used in security exploits. In total, the RiskIQ survey scans encountered more than 260,000 web assets and 1,777 individual mobile apps.

### DIGITAL FOOTPRINT BREAKDOWN OF LEADING FINANCIAL SERVICES CUSTOMER



## WEB THREAT RESULTS

Threats to a bank's web presence can come from a number of attack vectors, all of which can execute attacks from outside of a bank's firewall. The vectors include:

- Using flaws and security holes in client-side third-party components like JavaScript libraries to distribute malware
- Exploiting flaws in the servers' hosting websites and web assets either directly or via a compromised component such as server-side scripting languages, code libraries or external services and tools incorporated into the site's architecture. Server-side languages used by bank websites were 49% Java, 42% .NET, 18% ASP, 13% for Coldfusion, and less than 10% for both Perl and PHP.[2]
- Attacking or diverting traffic between users and the bank, such as man-in-the-middle or web pharming attacks, via broken SSL certificates, bugs in communications layers like the Heartbleed bug in Open SSL, DNS corruption to redirect traffic, or email phishing to impersonate a bank's communications
- Compromising an external web asset like a PDF file, image file or other content. These widely distributed assets are hard to audit and secure at the same level as internally hosted assets. Outside of controlled ASNs, assets are most likely managed by third parties on servers that may not be securely maintained or patched. This is often the case even when servers were originally set up by the bank's IT group and is even more likely when the servers and assets were inherited via mergers and acquisitions.

## OF THE MAIN WEB DOMAINS FOR THE 35 BANKS SURVEYED BY RISKIQ:

- **61%** of the of the 260,000 surveyed web assets were stored—potentially unsecured—on external servers outside of IT department control. Only 39% of web assets were hosted on the bank's main web ASN where they are more easily secured and audited.

- **94%** of the surveyed bank sites had one or more analytics or tracking services embedded in their websites that may pose security risks. For example, Gigya was hacked by the Syrian Electronic Army (SEA) in November 2014 using a DNS redirect, leading to website defacement of a number of well-known commercial sites.[3]

- **94%** had one or more JavaScript libraries with an average of seven JavaScript libraries per bank. These types of client-side scripting languages are common attack vectors. For example, jQuery, the world's most used JavaScript library, has been attacked numerous times.[4]

- **97%** of the bank websites had a minimum of 13 broken SSL certs with 54% having more than 100, and with roughly twice as many errors on sites hosted on outside ASNs. Broken SSL certs allow attackers to perform man-in-the-middle attacks and fail to prevent domain squatters from hijacking known URLs to redirect unsuspecting users to their pharming websites.

- **93%** had assets hosted with cloud-based IaaS providers, such as Amazon Web Services or Rackspace. These hosted resources may not be under the control of the bank's IT department and are often set up and forgotten about or may be contaminated by malware originating from cyber criminals. Based on prior work with RiskIQ customers, an average of 40% of these assets are unmanaged.

## MOBILE THREAT RESULTS

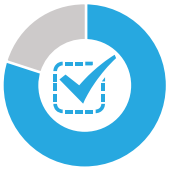
RiskIQ's survey also showed that many banks have much greater exposure to mobile threat vectors than might be expected. Mobile threats come from both security gaps in a brand's mobile apps and an uncontrolled proliferation of third-party apps, both legitimate and criminal in intent, that leverage a bank's brand to gain exposure to its customers.

Mobile app threats and vulnerabilities include:

- Security holes in components, libraries or services incorporated into apps
- Spoofing of the bank's brand by unauthorized third-party apps
- Unsecured, unpatched or out-of-date apps delivered outside of established app stores
- Excessive permissions required by both authorized and third-party apps

## THE SURVEY FOUND A TOTAL OF 1,777 MOBILE APPS PRODUCED BY OR ASSOCIATED WITH THE 35 BANKS:

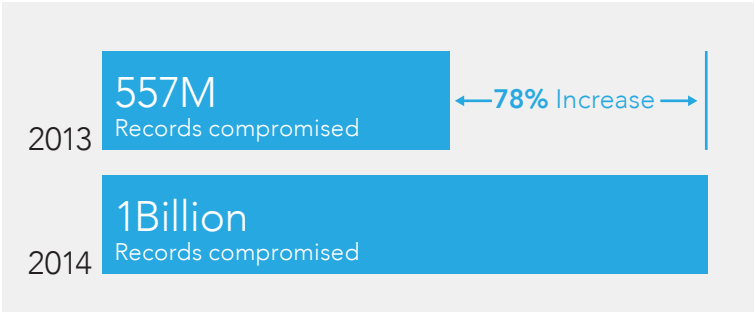
- **Only 6%** of the surveyed apps were hosted in official mobile app stores such as Google Play, Apple App Store, Amazon App Store and the Windows Phone Store. The other 94% were scattered through a secondary tier of app distribution sites, making it difficult or impossible to tell if updates or security patches would reach customers.



- **80%** of the discovered apps required users grant them 10 or more permissions, typically in excess of what was needed for app functionality. These permissions often grant unnecessary access to functions such as a user's contacts or a recording tool. This leaves an opening for any insecure third-party component used in the app to compromise the user's device. Although app users are asked to approve these permissions, they commonly just click "Accept" without knowing if it is safe or reasonable to do so.

## RECENT BREACHES CONFIRM SURVEY RESULTS

Large security breaches recently reported in the banking industry highlight the fact that these threats are not just theoretical. In 2014, worldwide data breaches across all industries increased 49% with almost 1 billion data records compromised in 1,500 attacks, a 78% increase over 2013.[5] While individual attacks are often fairly small, they quickly add up. For example, in February 2015, the Carbanak group had reportedly stolen more than $1bn in the past two years from up to 100 banks worldwide.[6]




Two recent attacks on bank customers that were executed from well outside the bank's firewalls include:

1. In 2014, the Dyre Wolf attack used sophisticated but automated social engineering tactics to gain access to depositor accounts. A spear phishing email was used to deliver the Upatre malware, which in turn downloaded the Dyre malware. Dyre then altered the display of a bank's website, tricking customers into calling a fake customer service number, which then captured their account credentials. Immediately afterward, an ordinary wire transfer is used to clear out the victim's accounts, followed up with a high volume DDoS attack to impede any investigation attempts by the victim. Not only did this approach not require any direct breach of the bank's networks, it completely side-stepped all of the two-factor and advanced authentication methods (i.e. more defense in depth) banks have added to their websites to secure customer sessions.[7]
2. In 2015, the Dridex banking Trojan used macro-infested XML files used by Excel that were attached to phishing emails posing as remittance or payment notifications. When loaded, these even used seemingly official popup notices to get unsuspecting users to defeat security barriers like disabling macros within Microsoft Office. Dridex ultimately loads a Trojan programmable to mimic a number of banking sites, capturing user credentials that are later used for the theft of funds. Again, this did not require breaching the bank's networks or firewalls.[8]

While these two examples of attacks were focused on bank web presences, the problem exists on mobile devices as well. An earlier survey by RiskIQ found that of 350,000 banking-related Android apps, more than 40,000—or 11%—were confirmed to contain malware or flagged as containing suspicious binaries from a consortium of 70+ AV vendors, with roughly 50% of those having signatures consistent with mobile-based Trojan malware.[9]

## PROACTIVELY ADDRESS THREATS

### MONITOR YOUR WEB ATTACK SURFACE WITH A REVOLUTIONARY APPROACH

RiskIQ Enterprise Digital Footprint discovers web assets, experiences them as a real user does, and allows you to accurately identify, monitor and manage your entire Internet attack surface from the outside in.

### DISCOVERY AND INVENTORY

- RiskIQ proprietary discovery technology recursively analyzes all the assets associated with your organization—and continuously discovers new, unknown assets—both legitimate and fraudulent ones.
- The technology accesses web assets and mobile apps by interacting as virtual users from around the world. This approach disarms evasion techniques used by malware to hide from traditional web crawlers and mobile app scanning agents.
- As the only company that sees the Internet from the perspective of the browser, RiskIQ sees what actually appears on social media pages, websites and mobile sites—just as it appears in users' browsers.
- The discovery technology captures the Document Object Model (DOM) and finds the dynamic links and changes made by JavaScript that could signify a potential attack.
- A dynamic inventory system provides full visibility into the state of all the assets for which your organization is responsible.

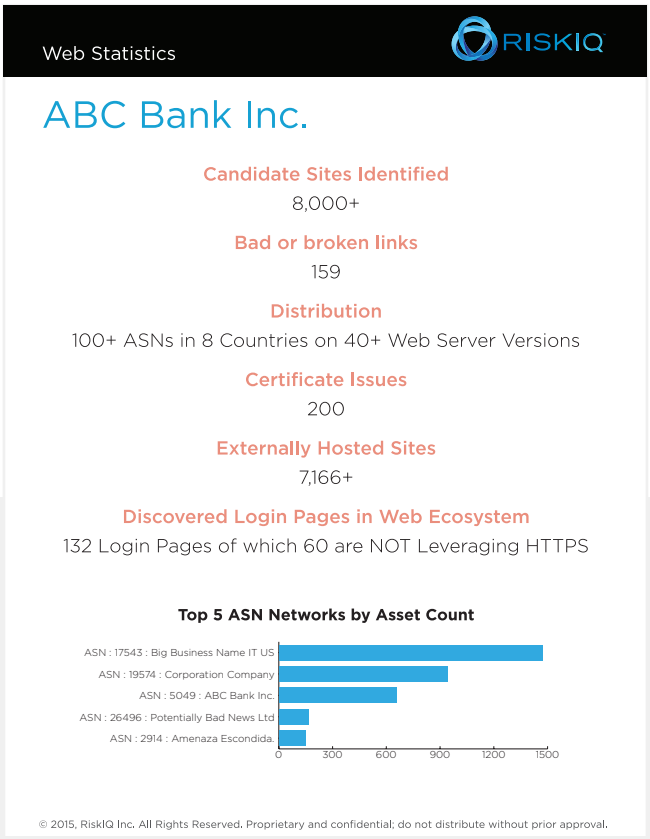
### REPORTING AND ENFORCEMENT

- RiskIQ provides a holistic view of the external threat landscape, at scale, enabling cross-team reporting and mitigation.
- A comprehensive, multidimensional view of assets enables accurate detection, fast remediation and proactive blocking of attacks.
- By illuminating what were formerly blind assets, RiskIQ allows you to apply policies to them and gain control.
- Industry scoring and vertical comparison tools offer the ability to compare your company's web asset security within your industry and against your competitors to see the best performing business units and report on ROI.
- By continuously monitoring the entire web at scale, RiskIQ technology can reduce personnel resources, improve accuracy, and minimize costs.

## HOW TO ADDRESS THESE NEW THREATS?

Like any other information-based industry that sells to consumers, banks face a broad range of threats that will never be addressable by any single silver bullet. Cyber crime scales up across the Internet with an ever-growing set of vulnerabilities exploited by increasingly sophisticated attackers. As the recent RiskIQ survey showed, the vulnerabilities outside your firewall already provide a rich playground for attackers, completely unencumbered by your internal defense in depth measures.

So how do you secure your firm's web presence, mobile apps and brand value? Internal vigilance and improved security practices on the website and mobile app fronts can reduce some risks. The first step is knowing your exposure—assessing the number and sources of potential vulnerabilities outside the firewall.




## GET YOUR PERSONALIZED SCORECARD

To help banks understand their security profile and risks, RiskIQ can put together a personalized scorecard from the results of the latest scans of related web assets and mobile apps. An example of a digital footprint scorecard is shown here. Contact RiskIQ at info@riskiq.com or visit trust.riskiq.com/digital-footprint-scorecard to get a personalized version reflecting the level of risk your bank is potentially facing.

## SOURCE

1 http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf

2 https://www.whitehatsec.com/news/14pressarchives/PR_041514_statsreport.html

3 http://www.scmagazine.com/syrian-electronic-army-redirects-gigya-briefly-compromises-media-sites-on-thanksgiving-day/article/385653/

4 http://www.riskiq.com/resources/blog/jquerycom-confirms-website-compromise

5 http://blogs.wsj.com/digits/2015/02/12/1-billion-data-records-stolen-in-2014-says-gemalto/

6 http://www.riskiq.com/resources/blog/massive-bank-heist-highly-sophisticated-attack

7 http://threatpost.com/dridex-banking-trojan-spreading-via-office-macros/110255

8 http://threatpost.com/dridex-banking-trojan-spreading-via-macros-in-xml-files/111503

9 http://www.riskiq.com/resources/blog/banking-customers-are-plagued-dangerous-mobile-applications

## ABOUT RISKIQ

RiskIQ provides organizations the visibility and intelligence they need to secure their known and unknown Digital Footprint. Using a global proxy network of virtual users, RiskIQ continuously discovers and creates an inventory of documented and undocumented web assets, and scans them for copycat mobile apps, drive-by malware and malvertisements. Leading financial institutions and both consumer and B2B brands use RiskIQ to protect their web assets and users from security threats and fraud. RiskIQ is headquartered in San Francisco and is backed by growth equity firms Summit Partners and Battery Ventures. To learn more about RiskIQ, visit **www.riskiq.com**.