WHITE PAPER

Why You Need to Protect Your Customers' Online Experience in Real time

An Osterman Research White Paper

Published July 2014

SPONSORED BY

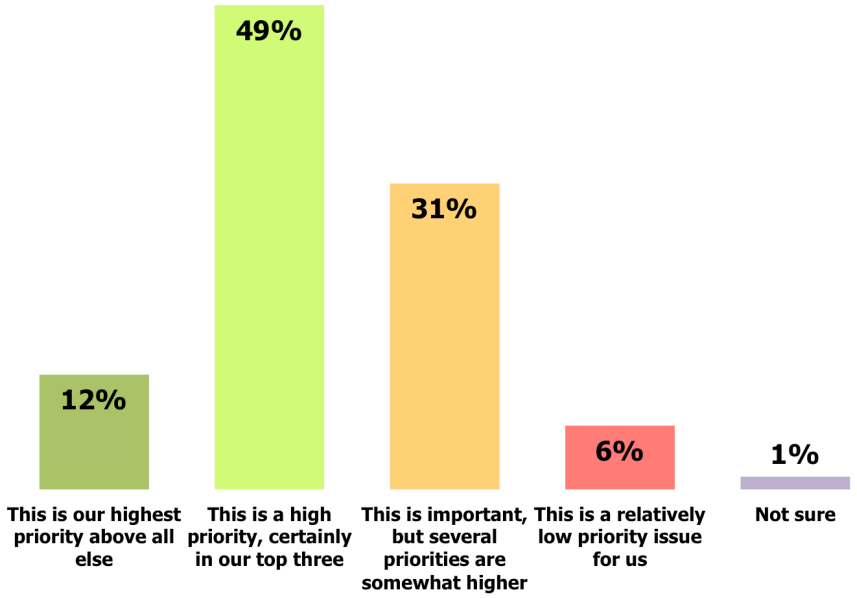
Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

THE GOOD NEWS

Many decision makers and influencers have placed a high priority on protecting their customers' online experience from malware, data theft and related types of problems. As shown in Figure 1, a significant majority of decision makers and influencers have made this their highest, or at least a top three, priority.

Figure 1
Importance of Protecting Customers' Online Experience



Source: Osterman Research, Inc.

THE BAD NEWS

However, most organizations are not doing enough to protect their Web and mobile properties from infiltration and so, by extension, are not doing enough to protect their customers. For example:

- The Identity Theft Resource Center (ITRC) recorded 614 breaches on its 2013 ITRC Breach List, an increase of 30% compared to 2012[i].
- Malware delivered through Web advertisements has increased by roughly 300% since 2012[ii].
- The number of risky or malicious Android mobile apps increased from slightly more than 500,000 in the first quarter of 2013 to one million during the fourth quarter[iii] of 2013.

WHAT DECISION MAKERS NEED TO DO

Clearly, any company that owns or manages a Web or mobile property needs to maintain robust security for these valuable assets. However, the fundamental and overriding goal should be the protection of its customers from malware infiltration, data theft, loss of sensitive or confidential information and other exploits that could harm customers and, ultimately damage its business and brand. Companies must monitor their Web sites for various threats that include malware and other malicious content like malvertising. They must monitor various stores that market their mobile apps to ensure that copycats and brand-stealers are discovered and shut down. They

Most organizations are not doing enough to protect their Web and mobile properties from infiltration and so, by extension, are not doing enough to protect their customers.

must monitor for malware in their mobile apps. Moreover, they must do so using an approach that a) takes into account the new security paradigm that many corporate assets are now housed outside the corporate firewall and far less under their control than they were just a few years ago, and b) that threats are changing continually and require a new approach if customers are to be fully protected.

ABOUT THIS WHITE PAPER

This white paper focuses on the increasing level of threat that any Web or mobile app customers faces and what companies must do to protect them. It also provides a brief overview of RiskIQ, the sponsor of this paper, and its relevant offerings.

CUSTOMERS ARE MIGRATING FROM THE SECOND TO THE THIRD PLATFORM

THE FOCUS IS SHIFTING

We are in the midst of the third generation of computing – what many call the "third platform":

- The first platform was characterized by the highly centralized computing architecture of the mainframe era, covering the era from the early 1950s to about 1985. During this era, customer engagement via any sort of "online" capability was non-existent, nor was cybercrime.

- The second platform, spanning the next 30 years from 1985 to about 2005, was characterized by the client-server era in which computing power became highly distributed. Despite the emergence of online customer engagement, threats to customers, data and assets were minimal compared to today's threat landscape.

- The third platform is characterized by an enormous growth in computing power housed in mobile devices, as well as by rapid growth of cloud computing, the Web and Web applications, Big Data analytics and social networking – and, most notably, a shift to an online customer experience. The third platform is focused heavily on customer engagement, increasingly via personally owned devices and applications that are outside the direct control of companies that manage the online experience.

In essence, the third platform represents both the best and the worst generation of computing: the best, in that users and companies are empowered like never before by highly capable applications, enormous computing power, and falling prices; and the worst, in that companies and their customers are now more vulnerable than ever before to cybercrime that can steal data, commit fraud, destroy brands and put companies out of business.

RAPID EXPANSION OF MOBILE, CLOUD AND WEB RESOURCES

Mobility and the cloud are arguably the most important issues impacting organizations of all sizes because of the enormous implications they have for IT and business decision makers in the context of security of, access to and control of corporate content. This rapid expansion of mobile and cloud resources is focused on providing internal capabilities for employees, the enablement of business partners and, most importantly, to serve customers.

Dramatically complicating the issue is the fact that a significant proportion of the applications, smartphones, tablets and other computing solutions that access corporate systems are outside the control of the companies that engage with their customers and their employees.

Obviously, the Web is integral to both increasing mobility and the growing adoption of the cloud to provide internal and external capabilities to employees, business

This white paper focuses on the increasing level of threat that any Web or mobile app customers faces and what companies must do to protect them.

partners, customers and others. The result of these sea changes in the computing environment is a massive increase in resources that are located outside the firewall – and a dramatic increase in the risks that organizations face on a growing number of fronts.

ONLINE CAPABILITIES ARE AN ESSENTIAL PART OF DEALING WITH CUSTOMERS

It goes almost without saying that online capabilities are an absolutely essential component of pre-selling to customers, the purchase process, providing customers with service after the sale, and retaining customers over the long term. For example, one study[iv] found that 62% of Internet-enabled consumers in the United States shop online at least once per month, while only one percent of these consumers indicate they would never shop online. Moreover the same study found that:

- 64% of consumers employ their mobile devices while shopping in traditional stores to research products.
- 59% of consumer would be more likely to shop at a traditional retailer if that retailer offered self-checkout capabilities using a mobile device.
- 42% of consumers would be more likely to purchase online if they had more confidence in online payment security.

What this clearly indicates is that a) not only are more consumers migrating to a direct, online sales model; but b) they want to integrate online capabilities with the traditional, in-store purchase experience; and c) they are being hampered in their pursuit of this improved sales model by a lack of confidence in the security of online sales.

THE RESULTS

This migration to online modes of engagement for sales, customer service and other business processes has created two interesting phenomena:

- A massive and growing proportion of computing resources and data assets that are now outside of the corporate firewall and, hence, outside the direct, physical control of commerce providers, corporate data managers, IT departments and others.
- Significantly more opportunities for cybercriminals to attack customers, steal data or otherwise infiltrate the online process for malicious purposes.

This migration to online modes of engagement for sales, customer service and other business processes has created two interesting phenomena.

PROTECTING THE CUSTOMER IS CRITICAL

YOUR CUSTOMERS ARE EXPERIENCING YOUR BRAND IN VARIOUS WAYS

There are several ways in which customers and others are experiencing online brands and the entire customer service experience via mobile applications and the Web:

- Through legitimate mobile applications and Web properties that are maintained by online sellers, information providers and others who provide various applications, services, online commerce and other capabilities.
- Through bogus mobile apps produced by cybercriminals that are designed to impersonate legitimate apps.
- Through bogus Web sites that, like fake mobile apps, are designed to impersonate a valid Web site offered by a legitimate brand.

- Through legitimate and active Web sites or Web site components (e.g., advertising banners) that have been infected by cybercriminals for the purpose of redirecting users to non-legitimate Web sites, infecting their computers with malware, or stealing data.

- Through hijacked Web pages that are maintained on corporate Web sites about which companies may no longer be aware. These may be customer-focused Web sites, employee-focused SharePoint sites, or Web-based applications that were once used for legitimate purposes, but that are no longer used, but have not yet been decommissioned.

CUSTOMERS ARE BEING EXPLOITED

As it is common practice to force users to accept permissions upon downloading mobile applications, fake mobile apps can come preloaded with a variety of permissions that grant access to a wide array of private data stored on phones (e.g., get accounts, read SMS, access contacts, access calendar, billing, etc.). Customers are trained to accept permissions without second guessing why some intrusive ones might be included, and thus unwittingly can offer the application provider, who may be looking to exploit them, free access to private data.

CUSTOMERS BLAME YOUR COMPANY AND YOUR BRAND, NOT THE BAD GUYS

Aside from the obvious problems of customers and others being exploited and having their financial data and personal information stolen, or having their computers infected with malware; these victims will often blame the company – or the brand associated with that company – for not doing enough to protect them.

For example, one of the most high profile data breaches was that of Target, which may have compromised the personal information of as many as 110 million of its customers in November 2013. A report from Kantar Retail[v] found that:

- 33% of US households shopped at a Target property in January 2014, the lowest figure in three years and a 22% drop from January 2013.

- During December 2013, the month following the breach, the number of Target shoppers increased by only three percent, not the typical 7-10% increase the retailer normally experiences during the holiday season.

Target was not breached, it's customers were breached.

Another study[vi], this one from Interactions, found that following a data breach 12% of a retailer's local customers will simply no longer shop with that retailer, 36% will reduce their shopping frequency, and 79% will be more likely to spend less at the retailer by using cash instead of credit cards. Making the problem even worse is that the survey found that 85% of victims will tell others about the problems they experienced at the retailer, while 34% will complain via social media channels.

Though the Target breach was executed through the point of sale system at the retailer, and not online, this breach offers a stark warning. Target was not breached, it's customers were breached. In the end, the customers were made whole, and Target lost millions in revenue and untold customer loyalty, while the CEO and senior security staff lost their jobs.

THE BOTTOM LINE

While most victims of cybercriminal activity will understand, at least intellectually, that a retailer, company or brand that is compromised via a bogus mobile app or a hijacked Web property is also a victim; the consumers who are the primary victims of the exploit will blame the company or brand to a much greater extent than they will cybercriminals. Consequently, companies must protect their data assets because their customers are the targets of cybercriminals. Ultimately, companies can protect themselves and their brands by protecting their customers.

WHY IS THE PROBLEM OCCURRING?

THE SECOND AND THIRD PLATFORMS ARE INEXPENSIVE AND EASY TO EXPLOIT

There are several reasons that new computing models based on mobile apps and the Web are easy to exploit:

- The Web is an open source environment for which security has been more or less an afterthought. There are ways to secure the Web, but these are necessarily "bolt-on" approaches because the Web was never designed with security as its primary goal.

- The number of Web sites is growing rapidly. For example, in 2008 there were 172.3 million Web sites, in 2011 there were 346.0 million, but by 2013 this number had grown to 673.0 million. As of this writing in late July 2014, there are 1.01 billion active Web sites[vii].

- The number of mobile apps is also increasing at a rapid pace. Canalys estimates that there are approximately 1.6 million apps available between the Apple App Store and Google Play stores combined[viii], although there are approximately seven million apps available as of July 2014. ABI Research estimated that in 2013 a total of 56 billion smartphone apps would be downloaded[ix].

Another enabler of cybercriminal activity other than the sheer size of the Web and mobile app market or the inherent lack of security of the Web is the fact that many Web and mobile asset owners make exploits relatively easy. For example, many asset owners will forget about their various Web and mobile properties and so will not recognize when they have been compromised. The code in these properties often is easy accessible and copied by cybercriminals intent on producing bogus versions of valid Web site and mobile apps. This results in the opportunity for cybercriminals to operate with few restraints as they work to exploit customers, employees and others.

Many Web and mobile asset owners make exploits relatively easy.

MALVERTISING IS A GROWING THREAT

As its name implies, malvertising is malicious Internet advertising that is used to distribute malware. The problem is an increasingly serious one because of the enormous impact it is having on users and brands. As noted in an Online Trust Alliance brief, a single malvertising incident can result in 100,000 impressions, with more than 10 billion malvertising impressions occurring in 2012 alone[x]. Underscoring the severity of the problem, a study by RiskIQ for the period January to September 2013 found that 42% of malvertising is carried out by drive-by exploits that require no interaction on the part of users[xi].

Malvertising can be hard to detect. For example, a cybercriminal might purchase ad space on a Web property and post a legitimate – or at least not a malicious – advertisement. A short time later they will replace this ad with a malicious one, but then switch back to the legitimate content after infecting a large number of visitors.

WEB SECURITY IS ESSENTIAL

Because the proliferation of Web properties is occurring rapidly, managing them is becoming increasingly difficult. Cybercriminals can exploit improperly managed Web properties and can cause serious harm to their owners. Exacerbating the problem is that conventional management of Web properties has become untenable without the appropriate solutions in place. For example, our research into a number of leading consumer-focused companies indicates that they have thousands of Web properties, each of which can have thousands of individual Web pages associated with them. One household name tech company has more than 10,000 different Web properties. Having such a large number of domain properties makes protecting them difficult, if not impossible, without the appropriate policies and technologies in place.

There are a number of ways in which cybercriminals can exploit improperly managed Web properties, including:

- Cross-site scripting attacks which embed various tags in URLs. When users click on these links, malicious JavaScript code can be executed on their computers.
- SQL injection attacks that occur when SQL commands and meta-characters are inserted into input fields on a Web site, which can then execute back-end SQL code.
- Cross-component attacks that occur when two seemingly harmless pieces of malware code appear on the same Web page. As separate components, they are harmless and difficult to detect, but when they appear on a single page at the same time they can infect a user's machine with malware.
- Cross-Site Request Forgery (CSRF) attacks that generate requests to various Web sites. CSRF attacks have been able to exploit vulnerabilities in Twitter, for example, enabling site operators to acquire the Twitter profiles of their visitors. Web 2.0 applications often leverage XML, XPath, JavaScript and JSON, Adobe Flash and other feature-rich internet applications. The result is that the applications are frequently vulnerable to injection attacks using these environments and can be used to evade anti-virus defenses.
- Search engine queries that can be hijacked by cybercriminals to distribute malware. This attack vector relies on poisoning search queries, which results in the display of malware sites during Web queries. Search engine poisoning is particularly effective for timely and popular search terms, such as the latest news about natural disasters or celebrities.

Malicious use of legitimate Web properties can occur through brute-force hacking into a Web site, or by placing malware on abandoned corporate Web pages and then directing victims there through phishing or other means.

Malicious use of legitimate Web properties can occur through brute-force hacking into a Web site, or by placing malware on abandoned corporate Web pages and then directing victims there through phishing or other means.

MALICIOUS MOBILE APPLICATIONS ARE PREVALENT

The growing use of smartphones and tablets is being exploited by cybercriminals. As just one example, customers of a major financial services firm have been targeted with a man-in-the-middle attack (a variant of Zeus) that will install malware designed to intercept passcodes sent to BlackBerry and Symbian devices via SMS as part of a two-factor authentication scheme[xii]. Moreover, mobile threats are increasing rapidly:

- During the first quarter of 2014, F-Secure discovered 277 new threat families, 275 of which were directed at Android, one at iOS and one at Symbian. Of the 277 threat families discovered, 91% were classified as malware[xiii].
- Sophos discovered an average of 1,000 new malware samples per day for the Android during 2013; so far in 2014, the company is discovering twice that number[xiv].
- Trend Micro has discovered roughly 647,000 new high-risk apps and mobile malware during just the first quarter of 2014[xv].

Complicating the problem is that there are a large number of third-party app stores like the Opera Mobile Store, Handango, Mobile Rated, Appitalism, Getjar and the Amazon Appstore for Android, among many others. While major stores like the Apple App Store, Google Play, BlackBerry World and others do a reasonably good job of trying to prevent malicious apps, some (but not all) third-party app stores are less diligent in protecting against threats.

THE CONSEQUENCES CAN BE SERIOUS

BRAND THEFT IS INCREASING

Brand theft is common on the Web and occurs in a number of ways: when domain names with similar spelling are registered by entities other than the trademark holder, when a registered trademark is used for a different product, or when the names of trademarked Internet properties are used as keywords for search engine advertising. Two examples:

- In late 2013, NQ Mobile reported a copycat mobile app designed to impersonate the legitimate NetDragon 91 Assistant app. Once installed, the copycat app will send premium SMS messages that will appear as additional charges on victims' wireless bills[xvi].

- The archiving firm Gaggle.net, Inc. received a trademark for the name "Gaggle" from the United States Patent and Trademark Office in April 2010. However, in April 2014 another firm unaffiliated with Gaggle.net posted the "Gaggle – Local Message Board" app to the Apple iTunes store and a few weeks later it was made available on the Google Play store. Gaggle.net has taken legal action to take down the app using its name, but has not been able to persuade either Apple or Google to do so[xvii].

- The secondary life insurance market is an industry that resells life insurance policies to investors. In 2011, someone opened a Twitter account, presumably intended for parody purposes, under a name quite similar to that of one of the leading participants in this market. The owners of the bogus Twitter account posted a number of tweets that the actual secondary life insurance provider found offensive. The company filed suit against the owner of the offending Twitter handle, alleging trademark and claims of unfair competition[xviii].

THE CONSEQUENCES ARE SERIOUS AND WIDESPREAD

There are a variety of consequences associated with brand theft, including customers who will no longer use a mobile app to purchase products or employ services from a compromised company, or customers who will no longer visit a Web site or purchase products from it for fear of having their confidential information stolen.

More strategically, however, a compromised company can suffer long-term damage to its corporate reputation and a permanent loss of customers who will refuse ever to do business with the company again. Moreover, it is important to note that corporate victims of cybercrime whose customers have been compromised are not just small or unsophisticated companies, but also very large organizations – such as Target – that either do not have the systems in place to monitor the various ingress points for cyberattack or do not appreciate the seriousness of the threat they face.

THE CONSEQUENCES CAN BE EXPENSIVE

The results of exploited customers can go far beyond simply the loss of business from offended customers whose financial information or data was lost. Regulatory agencies and courts can impose fines or other sanctions on companies that do not sufficiently protect customer data. For example:

- D.A. Davidson & Company was fined by $375,000 by the Financial Industry Regulatory Authority (FINRA) for "its failure to protect confidential customer information by allowing an international crime group to improperly access and hack the confidential information of approximately 192,000 customers.[xix]"

- Columbia University and New York and Presbyterian Hospital inadvertently disclosed the electronic Protected Health Information of 6,800 individuals, violating the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The firms were fined $1.5 million and $3.3 million, respectively[xx].

A compromised company can suffer long-term damage to its corporate reputation and a permanent loss of customers who will refuse ever to do business with the company again.

- A data breach of 2.4 million Schnucks Markets' customers in 2013 resulted in an expensive settlement for the company: up to $1.6 million in reimbursement for customer expenses, up to $635,000 for plaintiffs' attorney fees, up to $300,000 for related identity theft losses, as well as miscellaneous other expenses[xxi].

CHANGES TO THE SECURITY PARADIGM ARE ESSENTIAL

THE MIGRATION TO THE SECOND AND THIRD PLATFORMS NECESSITATES A CHANGE IN THE SECURITY MODEL

The first platform faced virtually no threats from cybercriminals – mainly because there weren't any. The second platform faced some level of threat from cybercriminals and bad actors, but much less than today because a) most data was maintained behind corporate firewalls and in other secure locations, and b) because the primary threat involved hackers that, by today's standards, would be considered hobbyists.

Perhaps the most fundamental change resulting from the migration to the third platform is that many resources are now beyond the firewall, managed on mobile devices, on personally controlled platforms, in the cloud, on the Web – and, perhaps most importantly – in the hands of customers. Moreover, over the past few years cybercriminals have become much more financially incentivized are now very well funded and organized. Virtually anyone can become a hacker by purchasing malware software development kits at relatively low cost. The result is that Web and mobile property owners are now targets of cybercriminals, cybergangs, organized crime syndicates and low-level hackers that can make a substantial amount of money from their efforts.

THE THREAT LANDSCAPE IS SHIFTING

It is essential to understand that the threat landscape for mobile and Web properties is shifting because of the volatile nature of the attacks directed against them. For example, Panda Security has found that 20% of all malware ever created was developed in 2013 alone[xxii]. Because threats are changing quickly, older threats that traditional solutions address simply are not used by cybercriminals any longer. Similarly, threats that are impacting customers today will not be an issue in the near future because criminals will simply have evolved their attacks to newer forms that conventional solutions do not address. The result of this rapidly changing threat landscape is that an appropriate defense requires a reactive and automated threat detection capability.

Threats that are impacting customers today will not be an issue in the near future because criminals will simply have evolved their attacks to newer forms that conventional solutions do not address.

WHAT DO YOU NEED TO PROTECT YOUR CUSTOMERS?

In order to protect customers from exploits – and ultimately to protect organizations from the resulting fallout from them – a threat detection capability must include a number of elements:

- It must be able to determine what is happening to customers in real time, not in an "after-the-fact" mode.
- The technology must be able to find exploits that are being delivered to a company's customers, not simply those that exist in the wild.
- The solution must provide deep inspection across all possible venues that cybecriminals might attack: mobile apps, active Web sites, inactive Web pages, and all other active, on-hold and deactivated properties.
- The technology must enable protection on every possible front, including malware infiltration via any mobile device or Web asset, fraudulent activity, copy cat mobile applications or data leakage.

The goal of a threat detection technology is to emulate the customer experience to the greatest extent possible in order to maximize the possibility of finding every threat across every possible venue. However, the ultimate business goal of changing the security paradigm is an economic one: make the Web and mobile threat vectors more expensive for cybercriminals by reducing the potential return from their activities.

WHAT SHOULD YOU DO?

UNDERSTAND JUST HOW SERIOUS THE PROBLEM IS

First and foremost, decision makers must understand just how serious the problems discussed in this white paper actually are. While decision makers may understand intellectually the severity of these problems, Osterman Research has found that many organizations take a somewhat reactive approach to security, waiting until a problem has occurred before taking corrective action. However, the new paradigm of highly distributed data, increasingly malicious threats, and more damaging consequences necessitates a proactive approach to security is needed.

EVALUATE YOUR CURRENT SECURITY PROCESSES AND INFRASTRUCTURE

Next, we recommend that organizations evaluate their current security processes and their overall security infrastructure. For example:

- What problems have actually occurred and why?
- How are Web properties protected from infiltration by malware?
- How are mobile users protected from mobile malware?
- How frequently are organizations monitoring for copycat mobile applications?
- Where are data leaks occurring?
- What are the consequences to the brand and the business from data loss?
- What mechanisms are in place for remediation against these threats?
- How quickly can a threat be identified, diagnosed and eliminated?

These are critical issues that every organization must address as part of a best practices approach to Web and mobile security.

DETERMINE WHERE DEFICIENCIES EXIST

A thorough evaluation of the existing security processes will reveal where deficiencies exist. This is essential so that decision makers can prioritize the most serious threats first and identify the most critical areas for security investment. Moreover, understanding where problems have actually occurred can help decision makers to address those issues that will have the most impact on customer retention, protection of the corporate brand(s), and the long-term viability of the business.

IMPLEMENT APPROPRIATE POLICIES TO MANAGE THREATS

Next, we recommend the creation of detailed and thorough policies that are focused on protecting customer and employee privacy in accordance with regulatory obligations; managing potential compliance violations; determining how sensitive and confidential data will be protected; managing the distribution of mobile apps; establishing a testing and security framework for all Web apps, mobile apps and other online assets; specifying how domain names will be managed; and determining how Web properties will be acquired, activated, deactivated and sold.

One simple example of how policies can help an organization to protect its brand is for the renewal of domain names. There have been numerous instances – some of them by very large companies – in which someone simply forgot to renew a corporate domain name. For example, in July 2014 Sony forgot to renew the domain name "sonyonline.net", which temporarily blocked user access to online games Landmark and Everquest[xxiii]. Microsoft forgot to renew the domain name "hotmail.co.uk" in late 2003[xxiv]. Yatra.com, the second largest online travel agency in

The new paradigm of highly distributed data, increas-ingly malicious threats, and more damaging consequences necessitates a proactive approach to security is needed.

India, booking about 6,000 reservations per day, forgot to renew its domain name in August 2013[xxv]. National Australia Bank forgot to renew the domain names for two of its banks in July 2013, thereby shutting off banking services to its customers[xxvi]. In many cases, organizations that neglect to do something as simple as renew a domain name a) do not have adequate policies in place to protect their Web and other properties, and b) probably have far more serious policy deficiencies.

DEPLOY THE RIGHT TECHNOLOGIES THAT WILL ALIGN WITH POLICIES

Finally, we recommend deploying the appropriate technologies that will enable an organization to adequately protect its Web properties and mobile apps, and – most importantly – will protect customers and employees from malware, phishing attacks, data loss, fraud and policy violations. Many technologies exist that focus on protecting the company and its data assets. However, technologies must be implemented that focus on protecting the customer – which ultimately will protect the company and its data assets.

ABOUT RISKIQ

RiskIQ™ is a leading provider of enterprise security solutions beyond the firewall. The company's proprietary virtual user technology intelligently interacts with websites and mobile applications, modeling end user behavior to trigger and detect anomalies, policy violations and previously undetected threats. A global proxy network scans millions of web pages and mobile applications daily, providing some of the world's largest financial and technology companies unprecedented visibility and control of critical assets distributed beyond their corporate borders

RiskIQ™ provides the following solutions to help companies address the problem of visibility and control of their web and mobile assets.

MOBILE APPLICATION SECURITY

As the number of mobile apps and the stores that distribute them come and go, it becomes a resource intensive challenge to maintain control of your apps across all these touch points. RiskIQ automates the discovery of what mobile apps exist representing your brand and over which app stores they are being distributed, With our automated discovery technology and our global threat intelligence spanning more than 7 million mobile apps over more than 90 app stores, we help companies identify immediate threats and automatically take down unauthorized apps using their brand or connecting to their IT systems.

WEBSITE SECURITY

With more than 4.5 billion pages across 650 million unique websites in existence today, it is a challenge to keep a pulse on one's web footprint and ensure the security of all associated web assets. With a unique approach to scanning the open web, RiskIQ can quickly determine an organization's ownership of web assets and their respective dependencies. Once these assets are discovered, they can be brought under management for continuous monitoring. Because of our expansive coverage of the web, we detect emerging threats before they can do major damage to a company's online brand.

MALVERTISEMENT AND MALWARE PREVENTION

Because there are so many players in the ad supply chain, websites that run third-party ads don't have much control over what ads are displayed to their visitors. RiskIQ intelligently scans and tracks advertisements as they traverse through the ad supply chain. We detect, classify and report on suspicious activity and confirmed malvertisements, notifying advertising operations team in real-time with detailed forensics of events uncovered.

www.riskiq.com
twitter.com/RiskIQ
info@riskiq.com
+1 888 415 4447

BRAND AND TRADEMARK PROTECTION

RiskIQ monitors the web for trademark misuse and abuse, prioritizing these incidents based on their monetary impact to a business and brand. Our comprehensive solution spans both emerging and targeted content -- the advertisements, blogs, mobile apps, and websites that have the greatest chance of reaching and influencing a company's current and potential customers.

REFERENCES

[i] http://www.idtheftcenter.org/images/breach/2013/UpdatedITRCBreachReport2013.pdf
[ii] http://www.bbc.com/news/technology-26447423
[iii] http://www.sys-con.com/node/2835260
[iv] http://www.marketingprofs.com/charts/2013/12195/online-shopping-trends-most-popular-categories-top-purchase-drivers
[v] http://www.cnbc.com/id/101475389#.
[vi] http://www.interactionsmarketing.com/retailperceptions/
[vii] http://www.internetlivestats.com/total-number-of-websites/
[viii] http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/e#lotsofapps
[ix] http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/e#lotsofapps
[x] https://otalliance.org/system/files/files/best-practices/documents/advertising_risk_evaluation_framework.pdf
[xi] https://otalliance.org/system/files/files/best-practices/documents/advertising_risk_evaluation_framework.pdf
[xii] http://www.pcworld.com/businesscenter/article/220223/advanced_zeus_trojan_hits_polish_ing_customers.html
[xiii] http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2014.pdf
[xiv] http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf
[xv] http://about-threats.trendmicro.com/us/security-roundup/2014/1Q/cybercrime-hits-the-unexpected/
[xvi] http://securitywatch.pcmag.com/mobile-security/317083-mobile-threat-monday-malicious-banking-apps-and-crafty-copycats
[xvii] https://www.gaggle.net/top-social-networking-sites-and-apps-kids-use/stop-the-gaggle-local-message-board-app/
[xviii] http://www.scribd.com/doc/57482188/Coventry-v-Does-11-Cv-03700-E-D-Pa-June-7-2011
[xix] http://www.finra.org/Newsroom/NewsReleases/2010/P121262
[xx] http://www.hhs.gov/news/press/2014pres/05/20140507b.html
[xxi] http://www.databreachlegalwatch.com/2013/10/schnucks-supermarket-chain-reaches-preliminary-class-action-settlement/
[xxii] http://www.pcworld.com/article/2109210/report-average-of-82-000-new-malware-threats-per-day-in-2013.html
[xxiii] http://www.npr.org/2014/07/18/332498727/the-last-word-in-business
[xxiv] http://www.theregister.co.uk/2003/11/06/microsoft_forgets_to_renew_hotmail/
[xxv] http://techcircle.vccircle.com/2013/08/12/yatra-com-site-went-down-as-the-ota-forgot-to-renew-domain-name-site-back-up/
[xxvi] http://www.computerworlduk.com/news/it-business/3461647/confirmed-clydesdale-and-yorkshire-banks-forgot-to-renew-domain-name/