50 Years of Growth, Innovation and Leadership

Managing Digital Risk

The Security Challenge Beyond Your Perimeter

A Frost & Sullivan White Paper

Jarad Carleton, Global Program Leader, Cybersecurity, and
Swetha Krishnamoorthi, Industry Analyst, Cybersecurity

FROST & SULLIVAN

CONTENTS

THE RELATIONSHIP OF DIGITAL TRANSFORMATION AND DIGITAL TRUST

Both enterprises and consumers are embracing digitalization, which is why connected device usage is at an all-time high and expected to continue growing. One result of digital transformation is that online transactions now make up over 50% of all Internet traffic making E-Commerce capabilities a necessity for every industry.

The general perception among global enterprises is that customers have confidence in the security of organizations they do business with online. Frost & Sullivan research on the Global State of Online Digital Trust paints a different picture.

The study revealed that average consumer digital trust index was a mere 61 out of a possible score of 100,[1] the equivalent of a failing grade. Consumer trust of companies has been declining, thanks to an alarming rise in the number of data breaches. Contrary to the belief of business executives, only 38% of consumers reported an increase in digital trust in organizations in the past two years.

THE CHALLENGE OF SECURITY BEYOND THE PERIMETER

Today, an enterprise has more digital touchpoints (Figure 1) to engage with customers and partners than ever before. Cyber-criminals exploit these touchpoints to trick people into sharing login credentials and personally identifiable information (PII). Not only are issues such as cyber-squatting a challenge, but organizations are also struggling to stay ahead of cyber-criminals who use APIs,[2] fuzzing,[3] link manipulation,[4] phishing through search engines,[5] and other techniques to make fake websites appear authentic.

1 Carleton, Jarad and Reed, Jason, "The Global State of Online Digital Trust" (Frost & Sullivan, 2018), 4.

2 Application programming interface definition—**https://www.sciencedirect.com/topics/computer-science/application-programming-interface**

3 Fuzzing attack explanation—**https://owasp.org/www-community/Fuzzing#**

4 Link manipulation explanation—**https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-part10.pdf**

5 Search engine phishing explanation—**https://medium.com/@ReputationDefender/tips-to-avoid-phishing-4-search-engine-phishing-bcaec7811933**

FIGURE 1: CONSUMER DIGITAL ENGAGEMENT TOUCHPOINTS

Source: Frost & Sullivan

Recent examples of the challenge beyond the perimeter are attack campaigns targeting Microsoft users that successfully led to the theft of log in credentials[6]. Cyber-criminals use techniques to clone organizations' branded Microsoft login pages. Such seemingly "legitimate" pages enable cyber-criminals to trick users into submitting their email address and password details on an attacker controlled site.

As CISOs and security teams are busy plugging enterprise security gaps at their perimeter, they seldom have security controls focused beyond their perimeter. However, a cyber-criminal can create a look-alike page with "HTTPS" security, with a seemingly legitimate domain name, and e-mail address. Unaware employees and customers rarely notice the difference between attacker controlled sites and the real thing. Furthermore, the use of exploit tools and automation to spin up and shut down attacker infrastructure enables fast moving attacks that are difficult for most organizations to discover let alone counter.

Enterprises generally work hard to implement security awareness training sessions for their employees. Often, enterprises attach annual performance metrics related to these sessions to increase awareness among employees. However, educating customers and partners can be much more difficult because they are not obligated to participate in phishing awareness training. Consequently, far too many people still cannot identify a sophisticated phishing attack that can result in stolen log in credentials and damaging theft of PII.

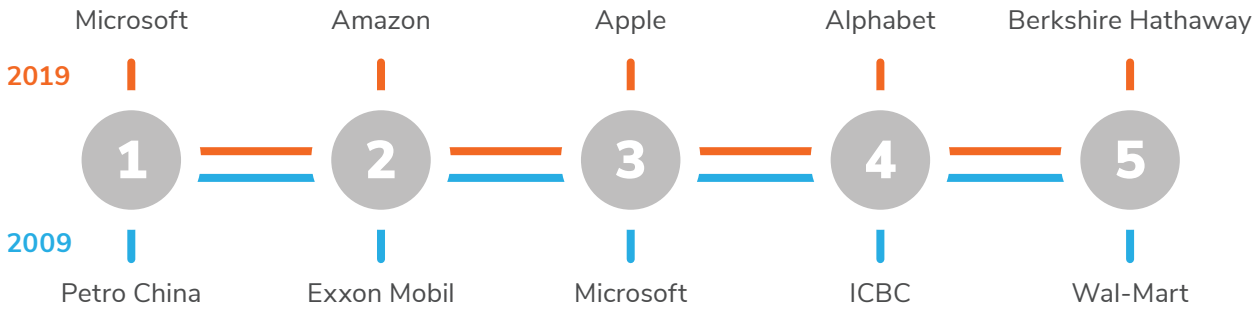
6 Gendre, Adrien. "Microsoft Again Most Spoofed as Office 365 Phishing Evolves." Security Boulevard, MediaOps, Inc., 21 May 2019, **https://securityboulevard.com/2019/05/microsoft-again-most-spoofed-as-office-365-phishing-evolves/**

CYBER-CRIMINALS MOVING FASTER THAN ENTERPRISE

The Case for Proactive Prevention

Data has become the most valuable commodity in the world[7] for companies of every size and in every geographic market. For that reason, companies with access to large volumes of data have the highest market capitalization (Figure 2).

FIGURE 2: TOP 5 GLOBAL LISTED COMPANIES, 2009 VS. 2019



Source: Financial Times and PwC

Conversely, data breaches are the second highest cause of brand reputation loss, next only to poor customer service. Because data is highly valued by businesses, it is also valuable to cyber-criminals who use creative means to steal it. People conducting business transactions online are becoming more wary of sharing PII and increasingly expect enterprises to have effective countermeasures against phishing emails and fake, brand exploiting websites. Organizations that are unable to respond quickly to threats beyond their perimeter will not be able to protect customers and data from falling into the hands of cyber-criminals. And while unfair, the legitimate brand owner will receive significant blame for the actions of the cybercriminals.

The Costs of Eliminating Threats with Manual Processes

The budgetary impact on an organization using manual processes to detect, investigate, and eliminate cloned websites can be significant. Because there is essentially zero unemployment for qualified information security analysts, market demand has driven the cost of these skilled professionals upwards[8]. Frost & Sullivan research on the global cybersecurity workforce has shown that a security

7 The Great Hack. Directed by Karim Amer and Jehane Noujaim. Interview of Brittany Kaiser, Netflix, 2019. Netflix. https://www.netflix.com/at-en/title/80117542

8 (ISC)2, "(ISC)2 Cybersecurity Workforce Study", ((ISC)2, 2018), **https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study**

analyst in the United States earns between 58 and 116 USD per hour depending on the state and level of experience.

Putting this into the perspective of digital risks, a medium sized enterprise using manual processes takes anywhere from 24 hours to 4 weeks or more of labor to scan the web to detect and take down a cloned website. This means, for every fraudulent website posing as a legitimate digital asset of a company, the targeted enterprise spends between 1,392 and 13,920 USD. A medium sized enterprise encounters an average of 6 clones per month. This number goes up as the enterprise size increases. Thus, every year, a medium-sized enterprise may spend between 100,224 and 1,002,240 USD in security analyst costs alone to discover and take down brand exploiting websites. Additionally, legal fees can cost as much as 2,000 USD per take down request, adding as much as 144,000 USD per year to online brand protection efforts. Lastly, hidden costs that will vary per company may include loss of business and potential regulatory fines that come with data leaks. In the end, the cost of inefficient online brand protection can surpass a million dollars per year for a mid-sized enterprise with a limited digital footprint.

DIGITAL THREAT PROTECTION (DTP) FOR ONLINE BRANDS—A FROST & SULLIVAN BEST PRACTICES PERSPECTIVE

CISOs invest time and resources on many defensive techniques including platform hardening, network monitoring, security awareness programs, and perimeter controls. While these layers are important, they are insufficient, as the vectors of an attack on businesses continue to expand.

Cyber-criminals have become highly skilled at cloning websites, social media account spoofing, domain infringement, and look-alike mobile applications to dupe customers, partners, and employees into sharing data. Investing in a Digital Threat Protection (DTP) solution is a best practice adopted by organizations that use online brand protection strategies to minimize brand exploitation risk. DTP technology continuously monitors digital channels – including, social media channels, and mobile applications – for malicious activity targeting brands and their customers. DTP platforms can also eliminate days or weeks of costly work associated with detecting and remediating threats to a brand's digital footprint.

> Cyber-criminals use exploit tools and automation to rapidly spin up and close down cloned digital assets in short bursts.

With in-house monitoring, information security professionals can scan digital channels for clones when they have time or when they receive a customer complaint. However, because of a shortage of experienced information security professionals, timely detection of cybercriminals impersonating a corporate brand is all too frequently a whack-a-mole[9] game of luck. Moreover, cyber-criminals use

9 Whack-a-mole definition—**https://www.lexico.com/en/definition/whack-a-mole**

exploit tools and automation to rapidly spin up and close down cloned digital assets in short bursts, usually closely coordinated with phishing campaigns. All too often, by the time security teams receive complaints from employees or customers, the web pages have disappeared, and have resurfaced later on different infrastructure.

With a dedicated DTP platform, an organization can automate monitoring and enable time constrained information security professionals to focus on other important tasks. This helps in early detection and proactive response to threats. Further, DTP automation can significantly improve an organization's mean time to detect (MTTD) and the mean time to resolve (MTTR) – two key metrics that are monitored by CISOs and their information security teams. In addition, enterprises can score and prioritize response actions based on risk levels each organization defines for itself.

The combination of focused expertise on prolific and specific class of attacks, combined with advanced machine learning algorithms, DTP solutions are capable of identifying sophisticated and fast moving attacks on of an organization's online brands.

A DTP solution significantly reduces MTTD and MTTR, which can make a meaningful difference for companies that understand the relationship of online brand protection, digital trust, and bottom line revenue growth. Using typical in-house techniques the MTTD for a website clone or other online brand infringement at a medium sized enterprise can take weeks or months and MTTR can take 2 weeks or more. This provides ample time for cyber-criminals to steal logins and as much other data as possible. With a DTP solution, MTTD drops to minutes and MTTR ranges from minutes to a couple of hours.

DIGITAL THREAT PROTECTION (DTP) BY MIMECAST

Mimecast is firm with large global operations, traded on NASDAQ, and with over 38,000 customers. **Mimecast Brand Exploit Protect** offers organizations a managed, cloud-based solution that protects them from brand exploiting websites, and in the process, helps brands build digital trust with their customers and business partners. Mimecast's solution monitors digital channels for attacks against a brand's online presence, investigates, and remediates threats via site takedowns faster than organizations can do on their own.

Mimecast Brand Exploit Protect provides holistic protection against external digital risks with a multi-step approach:

Pro-active Intelligence

This involves scanning the web around the clock, 24/7/365, for impostors and look-alikes to a customer's brand. The process includes scanning beyond the perimeter, across domain registrations, newly issued certificates and other potential digital touchpoints.

Threat Detection Agent

With a powerful web scraping tracker added to the customer's webpage in a way no one can spot, Mimecast detects any duplication or manipulation of the customer's website. The web scraping tracker detects both brand and non-brand related threats using dynamic or static content scraping.

Leveraging unique technology and machine-learning algorithms, Mimecast has been able to detect threats up to 48 hours before an enterprise information security team can.

Remediation

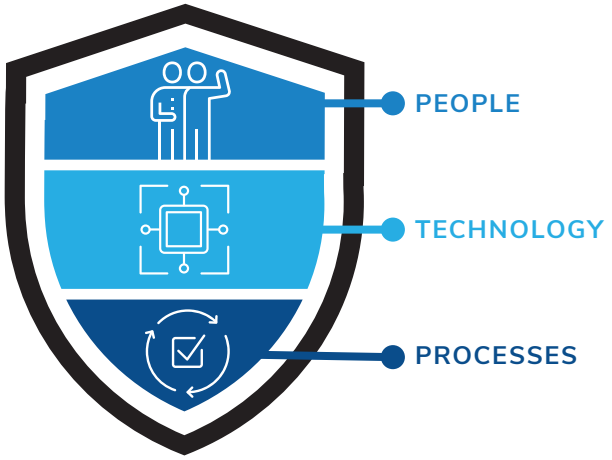
Remediation is faster and more effective than sending emails and letters to registrars requesting a takedown. Mimecast maintains strong relationships with stakeholders including registrars, hosting providers, certificate authorities, and others. Further, Mimecast has dedicated APIs for providers and has automated the takedown process with many infrastructure providers.

Mimecast's managed service model provides customers with a dedicated team of cyber analysts who follow up with the hosting providers to accelerate the remediation process. Thus, Mimecast is able to successfully takedown fraudulent sites within 3 hours, on average, and in some cases infringing sites are taken down in seconds.

> Mimecast's mitigation tactics have reduced number of clones to zero for the last 3 months.
>
> IT Security Manager—European bank

THE MIMECAST ADVANTAGE

Countering digital threats requires a holistic tripartite approach combining people, technology, and processes. Mimecast's digital threat protection platform enables businesses to protect their digital touchpoints beyond the company perimeter. The financial advantages of replacing a manual and time-consuming program to investigate and take down fraudulent sites are clear. Mimecast's managed solution provides measurable budgetary advantages when compared with most in-house online brand protection initiatives (Figure 3).



Source: Frost & Sullivan

> Mimecast's fully managed service costs significantly less than our in-house solution.
>
> IT Security Manager—European bank

FIGURE 3: THE ANNUAL BUDGETARY ADVANTAGE OF MIMECAST BRAND EXPLOIT PROTECT

Attribute	MANUAL Online Brand Protection: In-House Security Analysts and Legal Resources	AUTOMATED Online Brand Protection: Mimecast Brand Exploit Protect
Mean Time to Detect (MTTD)	Several weeks or months	Between seconds and 3 hours
Mean Time to Resolve (MTTR)	336 hours or more (2+ weeks)	Between seconds and 3 hours
Number of Customer-side Analysts Involved	5 to 20	1 analyst/10 minutes (telephone call)
Hours Spent on Online Brand Protection	160 hours per month	1 hour per month
Monitoring Frequency	Sporadic/when time allows	24/7/365
Web sites evaluated/year	Thousands/year	Billions/year
Cost per attack	Up to 13,920 USD	Up to 1,000 USD
Cost to monitor & protect 1 domain/year	Up to 1,002,240 USD	Between 12,000–60,000 USD
Annual Legal Fees/year	Up 144,000 USD	0 USD

Source: Frost & Sullivan

> Outsourcing to Mimecast has improved our customer satisfaction levels and brought downtime and resources utilized in digital risk protection to zero.
>
> Head of Cyber-Defense & Information Security—Multi-Asset & Brokerage Firm

FINAL WORD

Countering digital threats cost-effectively and protecting online brand reputation is a challenge for businesses. In-house teams using manual tools will rarely be able to work fast enough to move the needle in the constant struggle to reduce mean time to detect (MTTD) and mean time to resolution (MTTR) metrics for attacks beyond the network perimeter.

The global business environment has changed significantly over the past decade. The value of data and online transactions for businesses and the increasing regulatory compliance issues associated with protecting data have become the new normal. Online impersonation of corporate brands can impact the bottom line when enterprises do not proactively protect their digital footprint beyond just their network perimeter. The four issues CISOs, CTOs, Information Security Directors and managers need to avoid:

Extended MTTD—using manual tools and valuable security analyst time (as well as customers) to detect brand infringement is inefficient and costly.

Extended MTTR—spending 2+ weeks of security analyst time to resolve each brand infringement gives too much time for adversaries to inflict brand damage.

Infrequent monitoring—adversaries can spin up and close down cloned sites in minutes, making 24/7/365 automated monitoring business critical.

Legal fees—expenses associated with legal counsel getting involved with site takedowns is a costly misuse of a limited annual budget.

The accuracy and speed of response are critical when it comes to protecting your brand equity, digital trust in your brand, and your sensitive data during and after digital transformation initiatives. However, budget constraints also require a solution to be cost-effective. Leveraging a managed digital risk protection service is a best practice more enterprises are using to reduce attacks outside their network perimeter.

FROST & SULLIVAN

SPONSORED BY

mimecast®

SILICON VALLEY | 3211 Scott Blvd, Santa Clara, CA 95054
Tel +1 650.475.4500 | Fax +1 650.475.1571

SAN ANTONIO | 7550 West Interstate 10, Suite 400, San Antonio, Texas 78229-5616
Tel +1 210.348.1000 | Fax +1 210.348.1003

LONDON | Chiswick Business Park, 566 Chiswick High Road, London W4 5YF
Tel +44 (0)20 8996 8500 | Fax +44 (0)20 8994 1389

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?