

WHITEPAPER

BD-BrandProtect Perspective:
Protecting the Integrity of Your Brand
from Online Risk Exposure

Authored By:

Kevin Joy, Vice President, Marketing
BD-BrandProtect

December 19, 2006

Table of Contents

Introduction.....	3
Brand Integrity at Risk: A Call to Action.....	3
Quantifying the Costs of Online Infractions.....	6
Securing the Value of Your Brand.....	8
Moving to a New Model of Brand Protection.....	9
Metrics for Performance Management.....	13
Conclusion.....	15

Introduction

In recent years, corporate Internet strategies have evolved so significantly that the Web is almost universally accepted as simply another channel for doing business. The trend towards e-commerce likely started with catalogue shopping firms such as J. Crew, L.L. Bean and Land's End, and evolved to include strictly Internet-based businesses such as eBay, Amazon.com and Travelocity. Today, however, countless traditional "bricks and mortar" companies have extended their reach to sell online – reducing operating costs and speeding up the delivery of goods in the process.

The trend is so pervasive, in fact, that the Census Bureau of the U.S. Department of Commerce estimates that, in the third quarter of 2006, U.S. retail e-commerce sales rose 4.5% from Q2 to reach \$27.5 billion. Similarly, according to comScore Networks, a global Internet information provider, the all-time record for daily U.S. online retail sales was set on November 27, 2006 when online sales totaled \$608 million. Even more notably, that record was broken a mere one week later, on December 4, when consumers spent \$647 million online in a single day.

Yet, despite the enormity of the numbers, industry watchers agree that there remains significant room for growth in the world of e-commerce. U.S. Census Bureau numbers verify that e-commerce sales in the third quarter of this year accounted for only 2.8% of total sales – underscoring the sales opportunities yet to be leveraged on the World Wide Web. Additionally, there is little doubt that product information available over Internet sites will continue to influence consumer-purchasing decisions in both online and offline markets.

Brand Integrity at Risk: A Call to Action

This migration of commerce to the Internet has not been lost on the criminal elements of our society. As much as the Internet has opened up new areas of opportunity for business enterprises, it has delivered an equal bonanza for fraud artists, organized crime and a cornucopia of scam artists who find new and effective ways to bring harm to those who have, through legitimate means, built their business.

According to security firm McAfee, criminal gangs have gone so far as to hire students and plant them inside of companies, charging them with the tasks of writing

computer viruses, committing identity theft and laundering money.¹ Due to criminal activities like these, as well as similar security breaches, the U.S. Federal Trade Commission estimates that more than 52 million account records were placed in jeopardy in 2005 alone.

There are numerous forms of identity theft and brand abuse that currently take place over the Internet. One of the most familiar is called "**phishing**", a practice in which scammers hijack well-recognized brands in an attempt to dupe consumers into disclosing personal or financial information. Although phishing attacks were historically limited to financial services organizations, they have begun to spread to other retail-based brands. For instance, this year phishers misappropriated such well-known brands as Coca-Cola and McDonald's by using their trusted logos to lure consumers into divulging secure information through bogus promotions and sweepstakes offers. In fact, according to recent estimates, a record 14,191 phishing Web sites were created in July 2006, mimicking an eye-popping 154 brands.

Yet, phishing is not the only form of brand abuse that takes place online. As criminals continue to recognize the value of high profile brands, the scale of online infractions becomes increasingly diverse. Some typical online infractions include:

- **Counterfeiting:** The World Customs Organization estimates that counterfeit goods account for \$512 billion in annual sales. The scale of counterfeiting operations is so vast that it accounts for 7% of world trade, and would be the world's biggest business if it were named a business.² While much of this activity takes place offline, the Internet has made it increasingly easy for cyber-criminals to sell fake goods to consumers around the world. The potential damage to profits is so severe that fashion designers Louis Vuitton and Christian Dior actually filed a lawsuit against eBay in France claiming the online auction site does not appropriately monitor sales of counterfeit goods.³
- **Web Traffic Diversion:** In this type of attack, scammers misappropriate the source code of a website, such as its domain name or meta data. Although invisible to the eye, this information can be used to "trick" search engines into

¹ "Internet gangs hire students for cybercrime", *ZDNet*: Peter Griffiths, December 8, 2006

² "Knockoff: The Deadly Trade in Counterfeit Goods", by Tim Phillips

³ "Dior and Louis Vuitton sue eBay", *WebUser magazine*: Quentin Reade, September 21, 2006

believing that a bogus website is, in fact, related to a legitimate brand. This enables unauthorized third parties to divert Internet traffic from the legitimate website to a mirror site, which may sell competing products or may even be entirely unrelated to your brand.

- **Unauthorized Associations:** These infractions occur when your company is inappropriately associated with questionable organizations or activities. For instance, an international entertainment company recently had its well-known cartoon characters recreated and featured on a range of online pornography sites. In addition to potentially exposing highly offensive material to young children, this infraction may have resulted in negative publicity and a loss of consumer trust. In another well-known incident, an Internet rumor pegged designer and urban outfitter Tommy Hilfiger as a racist – a false rumor that still prompted some groups to threaten to boycott Hilfiger products.
- **Third-Party Compliance Issues:** Many of the infractions that take place on the Web are not criminal activities at all, but are committed inadvertently by authorized resellers, dealers and agents. Despite being unwitting, these infractions often bear a serious cost to organizations. For instance, in one case, authorized resellers of a global automobile manufacturer were featuring famous songs on their websites, without a proper license, to promote corporate products. This lack of compliance from its own channel saw the company presented with a demand for significant royalty payments.
- **Web Linking Infractions:** These infractions occur when a link appears on a third-party page, implying that a formal relationship exists between the two parties mentioned. These infractions are often more insidious than they appear, as was evidenced by one organization that began to receive hundreds of angry phone calls when its brand was inappropriately linked to a Neo-Nazi website.
- **False Job Postings:** In this type of attack, fraudsters post unauthorized employment listings that misrepresent a brand and create false job notices for the purpose of capturing personal information such as names, addresses, phone numbers and SSN information. In addition to compromising the ability of Human Resources departments interested in posting legitimate employment notices, this

practice creates the risk of brand deterioration and puts consumers at risk of becoming the victims of fraud or identity theft.

- **Cybersquatting:** In this form of online extortion, scammers buy and register a domain name with the intent of profiting by reselling it to a person or trademark owner at an inflated price.
- **Typosquatting:** This infraction refers to the practice of intentionally misspelling a trademark, using a variation of that trademark or using that trademark in conjunction with other content in the hope of confusing consumers and diverting them away from a legitimate website. This form of brand misrepresentation is illegal and can be mitigated.

Quantifying the Costs of Online Infractions

There is ample anecdotal evidence that online infractions threaten brand integrity, damage corporate reputation, result in lost revenue and lead to deteriorating customer loyalty. Yet the repercussions extend far beyond unquantifiable loss. In recent years, numerous research organizations, advocacy groups and media sources have released figures that measure the cost of online breaches in financial terms:

- According to a Gartner Group survey of 5,000 online U.S. adults in August 2006, 46% say that concerns about theft of information, data breaches or Internet-based attacks have affected their purchasing payment, online transaction or e-mail behavior. The research firm estimates the financial cost of this mistrust is approximately \$2 billion in 2006.⁴
- Gartner goes on to estimate that phishing attacks alone will cost U.S. businesses and consumers a whopping \$2.8 billion this year, with an average “take” of \$1,244 per victim.⁵
- According to a Ponemon Institute study, companies experiencing a data breach spent an average of \$14 million on recovery costs, including unbudgeted spending for outside legal counsel, mail notification letters, calls to individual

⁴ “Trust Has Value in E-Commerce”, *eMarketer*: Ben Macklin, November 30, 2006

⁵ “Who or What Is ‘Rock Phish’ and Why Should You Care?”, *PC World*: Robert McMillan, IDG News Service, December 12, 2006

customers, increased call center support and discounted product offers. Even more significantly, businesses that experience a data breach lose an average of 2.6% of their total customer base.⁶

- A poll of more than 2,000 North American and European consumers conducted by Opinion Research Corporation found that 59% of consumers would either strongly consider or definitely take their business elsewhere if their personal information was compromised.
- Media coverage of security breaches is also affecting brand integrity. According to Factiva, a Dow Jones and Reuters Company, media coverage of companies that suffered a security breach in 2005 accounted for more than half the stories written about those companies.
- Most significantly, an Emory University study recently confirmed that security breach events directly affect stock performance. When such events are reported, companies lose an average of 0.63% to 2.1% value in stock price – equivalent to a loss in market capitalization of \$860 million to \$1.65 billion per incident!⁷

The Internet is a largely ungoverned, open system that has proven to offer equal opportunity to both legitimate business concerns and criminal operators. Victims of fraud cut across all social, economic and cultural lines. Even affluent members of society can be victims of fraud, as criminal activity does not discriminate between rich, poor or middle class.

Online infractions don't just affect customers either. They can also cause mission-critical stress in your call center, damage your brand reputation and put your organization in a defensive mode. They diminish the potential of the Internet for e-commerce and undermine Information Technology investments. They also compromise customer relationship management by misrepresenting legitimate brands, ultimately putting confidential customer data at risk.

⁶ "Secure the Trust of Your Brand: How Security and IT Integrity Influence Corporate Reputation", A CMO Council Report, September 2006

⁷ *Sic*

The evidence is clear. The open, largely undefended market environment of the Internet has given rise to a variety of activities that impair a company's ability to optimally leverage its brand over the Internet. Online attacks lead to lost traffic, lost revenue and customer dissatisfaction. They also expose organizations to potential legal liability. According to legal experts, if a company is made aware of scams using its trademarks, and does not act to protect consumers, it could be held responsible in court for negligence.

"Phishers Switch Brand Bait to Coke and McDonald's", Advertising Age: Kate Macarthur, December 11, 2006

Securing the Value of Your Brand

The financial costs of online infractions continue to rise when you take into account their effect on the value of your corporate brand. Companies that are typically targets of Internet-based crime are often well-known corporate brands. Many are household names that are used every day by millions of customers who trust those brands and believe they identify those companies as hallmarks of ethical behavior. Most critically, these corporate brands are 'intangible assets' that go largely unprotected outside of a corporations' firewalls and security nets, despite possessing extremely high value in financial terms.

In fact, the financial value of a corporate brand as an intangible asset can and has been measured, as can be seen below in Figure 1. In the classic marketing sense, the corporate brand mirrors the identity of the corporation. 'Brand' is the essence of the corporate personality – who it is, what it stands for, its culture, values and role in the community. From a customer's perspective, the brand represents all of the promises of performance in shaping the customer's experience with the products or services that the brand represents across all touchpoints and channels.

Think of a number of examples: sugar and carbonated water, gasoline, bottled water, a computer chip or a car rental service. These products are essentially made from virtually unlimited resources but have distinct identities in our economy and social fabric – Coca-Cola, Exxon Mobil, Intel, Evian and Hertz. None of these brands came to prominence overnight. Their success as world-leading brands is in part a

function of astute long-term marketing, a deep sensitivity to customers' wants and needs, a transcendence from being economic entities to cultural icons and the ability to transform ideas into strategy through execution and a global presence.

Figure 1: Measuring the value of a brand

Top Global Brands		
According to Interbrand for Business Week, August 2006		
Brand	2006 Brand Value [\$millions]	Sector
Coca-Cola	67,000	Beverages
Microsoft	56,926	Computer Services
IBM	56,201	Computer Services
GE	48,907	Diversified
Intel	32,319	Computer Hardware
Nokia	30,131	Telecom Equipment
Toyota	27,941	Automotive

Source: Interbrand for Business Week, August 2006

What is clear is that each of these brands – and many others – have economic value. Their value is not just in their ability to attract customers and generate revenue today, but in their ongoing ability to generate a solid stream of revenue well into the future. Arguably, each time your brand integrity is threatened by online attacks and infractions, your ability to earn an ongoing stream of revenue over time is compromised.

Moving to a New Model of Brand Protection

Not unlike terrorism, online attacks, identity theft and Internet fraud can never be completely defeated, only mitigated. This requires a continuous commitment on the part of organizations to be vigilant by not only investing in appropriate technologies but also by building a culture of awareness, designing business policies and processes to combat online infractions and becoming cognizant of the damage that can be inflicted on both corporate brands and customer trust.

In today's heightened regulatory environment, organizations must attest to the effectiveness of their internal processes. As a result, there is now an urgent call to action for companies to immediately establish an enterprise-wide state of readiness to combat Internet fraud, reduce the severity and levels of online brand abuse and mitigate the financial harm to customers and the collateral reputational risk to the corporate brand.

In adopting this new model of brand protection, there are certain industry best practices to keep in mind:

- According to a comprehensive report released this past September by the CMO Council, a not-for-profit global think tank, a key strategy for securing brand integrity involves the adoption of consistent security and privacy policies across the enterprise. This means executives at every level of the business must come together to protect the brand at an enterprise level.
- The report goes on to identify three critical actions organizations must take to preserve brand trust. In a nutshell, companies are urged to: (1) Prevent infractions by implementing the right technologies and security policies; (2) Communicate openly and proactively with customers, business partners, shareholders and the press in the event of security breaches; and (3) Put a plan in place to help victims who are affected by online infractions.

These industry best practices are captured by the Brand Protection Roadmap set out in Figure 2:

Figure 2: Roadmap to establish a state of enterprise readiness



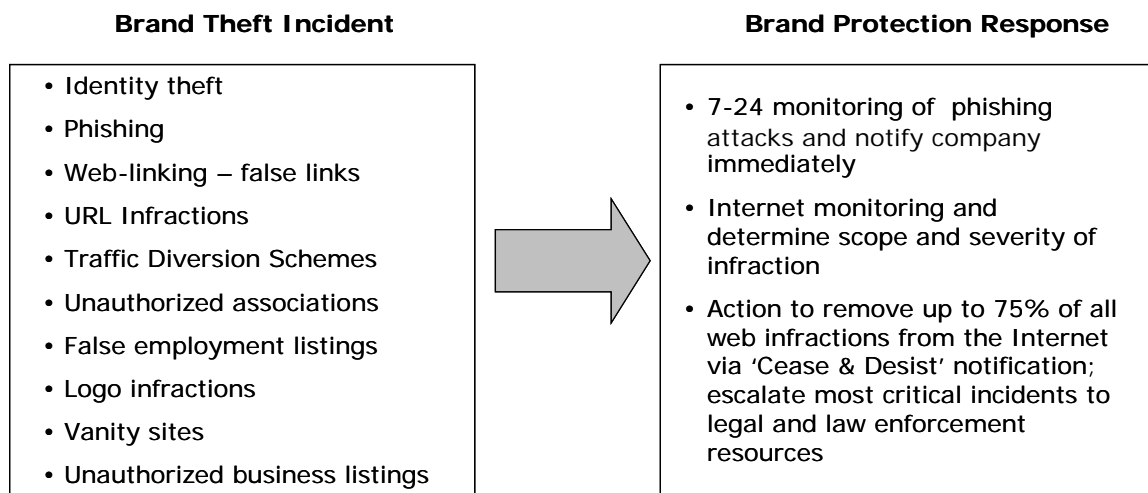
In essence, this strategy postulates that certain policies, processes and procedures should be established in the early stages of a brand protection program to ensure a high probability of success. An effective brand protection strategy should contemplate such issues as resource and process requirements, timelines, deliverables and expected outcomes, and often includes the following elements:

1. The establishment of an Internet Brand Protection Council with representation from, but not limited to, the following stakeholder groups: Marketing, Branding, E-business, Human Resources, Public Relations, Corporate Legal and Security & Fraud. The objective of bringing together this cross-functional group is to ensure that a philosophy of brand protection is instilled throughout the enterprise among all key stakeholders.
2. The development and implementation of brand protection policies and response processes based on corporate risk management strategies. By adopting a defined set of procedures, companies can reduce the impact of online brand attacks and minimize the potential damage they might otherwise suffer.
3. Corporate training to foster a culture of asset protection. Training documentation should include information on how to implement a response process, how to identify online brand abuses and how to report brand abuse attacks. It can also set out tactics for communicating with key stakeholders in the event of security breaches.
4. Baseline metrics that enable an organization to measure project success and quantify the benefits that accrue from a brand protection strategy. With appropriate metrics, companies can begin to align their online brand protection processes with their enterprise-wide performance scorecard to measure the extent to which the business benefits by the elimination of online threats.
5. Customer satisfaction metrics that enable an organization to gauge its service provider's contribution. Through this type of ongoing assessment, companies can intelligently determine if their online protection service providers are delivering the full anticipated value.

One of the primary objectives of an effective brand protection program is to enable organizations to establish long-term policies, strategies and processes that involve cross-functional participation to improve online asset management.

With this type of long-term corporate focus on risk management and prevention, companies can often minimize the damages resulting from online criminal activity, as illustrated in Figure 3.

Figure 3 – Collaborative proactive brand protection



To gain access to these benefits, however, it's important for organizations to look for service providers with a key set of capabilities, including:

- Best-of-breed detection services to scan the Internet for instances of online brand abuse, detect infractions no matter where they're located and determine their strength and influence.
- Proprietary filtering technology to filter the data captured and identify only the infractions that matter most to you.
- A robust human data analysis process to ensure all information you receive is prioritized, rather than simply "dumped" into an online portal.
- Global takedown capabilities that ensure offending site owners are contacted and Cease & Desist communications are sent in a timely manner to ISPs, upstream providers and CERTs around the world.

- The provision of post-incident forensics ranging from trace routing, WHOIS IP addresses, commentary logs, cached site copies, data stamps, details of steps taken to remove or eliminate brand infractions and a CD of historical information that can be sent to law enforcement agencies to prosecute cyber-criminals.

As the CMO Council report states:

“A company’s reaction to a breach affects the brand trust, which is why marketers must generate comprehensive response plans. A company that delays its response to a breach, provides vague statements, or refuses to comment altogether only increases that damage to its reputation that began with the breach itself. A response plan should be designed to demonstrate, quickly, clearly and publicly, that a company is fully committed to addressing the problem and undoing any real or potential damage to customers.”⁸

Metrics for Performance Management

When adopting an online brand protection strategy, a final issue to consider is the availability of robust performance metrics that enable you to measure the effectiveness of the approach at an enterprise level. In this way, companies can assure that the business value of protecting their brands and various intangible assets gets measured, acted upon and assessed by executive management.

For most organizations, experience shows that the most common forms of online infractions are likely to occur on an ongoing basis, rather than as isolated incidents. From a managerial perspective, then, it is important to design and manage these infractions via a corporate performance scorecard that is aligned with the corporate ‘balanced scorecard’. Metrics must be calibrated in a way that will help determine the business value of the harm being brought to the brands and defined in such a way that is meaningful to the stakeholder groups represented on the cross-functional brand protection council.

⁸ “Secure the Trust of Your Brand: How Security and IT Integrity Influence Corporate Reputation”, A CMO Council Report, September 2006, page 21

The most actionable metrics and scorecards are simple and easy to read by frontline employees, middle managers and executives alike. They do not simply provide a tally

of brand abuse, but track the level of severity, incidence levels and cost to the organization in the form of lost revenue, lost 'shopping intenders' and recovery costs.

The best metrics include associated actions and rates of success in mitigating brand abuse and fraudulent activity. This is where the executive management will be most interested in the process to protect the brand and evaluate the business value of the brand protection process in and of itself. The best case will deliver a true ROI measure; in the least, specific actions and outcomes will be tracked and measured. Realistically, most companies should strive to mitigate as much of the most harmful damage as possible, allocate resources to the most harmful activities and take steps to educate customers and employees alike about the various forms of Internet-based criminal activity. In this way, companies can begin to protect the integrity of their brands by mitigating and managing their online risk exposure.

Figure 4: Sample performance dashboard

ACME TELCO													
Sample Dashboard Report - Monthly													
ACME Brands	Websites monitored	URL Infractions				Traffic Diversion Schemes				Weblinking Infractions			
		Critical	High	Medium	YTD	Critical	High	Medium	YTD	Critical	High	Medium	YTD
Global Voice	948	0	1	0	1	0	7	0	7	0	6	105	111
Global Data	361	0	0	0	0	0	0	0	0	0	0	20	20
Global Internet	948	0	1	0	1	0	0	0	0	0	1	53	54
Local Voice	1,045	0	0	0	0	0	0	0	0	0	2	14	16
Local Data	413	0	0	0	0	0	0	0	0	0	0	4	4
Local Internet	138	0	0	0	0	0	0	0	0	0	10	20	30
PCS Group	1,048	0	0	0	0	0	0	0	0	0	0	12	12
ACME Brands	Websites monitored	Counterfeit/Misrepresentation				Compliance				Associations/ Listings			
		Critical	High	Medium	YTD	Critical	High	Medium	YTD	Critical	High	Medium	YTD
Global Voice	948	0	4	107	111	0	0	4	4	0	0	107	107
Global Data	361	0	0	14	14	0	0	0	0	0	0	1	1
Global Internet	948	0	1	20	21	0	0	3	3	0	0	29	29
Local Voice	1,045	0	1	16	17	0	0	0	0	0	0	29	29
Local Data	413	0	0	0	0	0	0	0	0	0	0	0	0
Local Internet	138	0	0	22	22	0	0	3	3	0	0	19	19
PCS Group	1,048	0	0	16	16	0	0	0	0	0	0	30	30

Conclusion

Before the rise of e-business and the Internet, criminals were mostly interested in stealing tangible assets. Similarly, business executives focused largely on building business value through the accumulation of tangible assets. The Internet has changed much of that, and has dramatically heightened sensitivity toward the value of the corporate brand, as it remains largely exposed and vulnerable on the Internet.

Without putting an appropriate online brand protection strategy in place, however, companies are at risk of compromising more than their brand reputations. As the statistics cited earlier note, they also face the very real threat of incurring measurable financial costs – ranging from lost sales and lost customers to a quantifiable erosion of market value.

By bringing online brand protection to the top of the corporate agenda, and implementing specific strategies, processes and measures to protect their brands, corporate executives can safeguard their hard-earned customer trust. At the same time, they can establish safe and effective strategies for leveraging the limitless opportunities offered by the Internet. This, in turn, can enable organizations to protect their online revenue streams, their customers' online experiences and their brand equity.

By identifying the appropriate brand protection partner, you can put a process in place to respond internally to online brand abuse. With this type of process in place, you gain the peace of mind of knowing that you are relying on industry best practices – and you free up your internal resources to remain focused on core competencies.

According to Forrester Research, there is a "... high correlation between perception of protection and revenue per customer". By working with a brand protection partner who understands your corporate priorities, leverages best-of-breed technological expertise, integrates human intelligence into the analytical process and responds proactively to attacks on your brand, you can begin to reap those tangible benefits while mitigating and managing your online risks.

About BD-BrandProtect

BD-BrandProtect, the leader in online threat protection, empowers organizations to gain control over how they are represented online by uncovering and mitigating the threats that put their reputation at risk and erode customer trust.

BD-BrandProtect is uniquely positioned to provide detailed and actionable reports on the most relevant and highest priority threats by combining advanced technology, round-the-clock monitoring, proven best practices and exhaustive human analysis.

BD-BrandProtect first scours millions of domains, Web pages and Internet links to uncover infractions. It then categorizes and ranks those threats according to their severity. It then initiates proactive and escalating response protocols to effectively mitigate threats when required

BD-BrandProtect has relationships with more than 2,000 Internet Service Providers globally that account more than 85% of the traffic flowing across the Internet. By consistently investing in this network, BD-BrandProtect customers have access to the most coordinated incidence response team ever created.

The company is recognized by many of the world's largest financial institutions as the leader in online threat protection. It serves the needs of a cross-section of organizations, including many of the world's most respected global brands.

BD- BrandProtect was founded in 2001 and is headquartered in Toronto, Canada, with offices in the United States, Singapore and London.

For more information: www.bdbrandprotect.com

About the Author

Kevin Joy, Vice President of Marketing, is responsible for all aspects of global branding and marketing for BD-BrandProtect. Kevin has over 16 years of marketing experience growing leading consumer goods and professional services firms. For the past 7 years, he has led the market strategy and program development of all

Deloitte Canada's services and played a major role globally as a member of the firm's marketing, communications and business development council, most notably as a leader of its branding initiative.

Prior to this, he spent eight years with Unilever in Canada and Mexico. In Canada, he built Becel into one of Canada's most successful and trusted household brands and then went on to lead Lipton's food innovation effort. While in Mexico, his experience included being an integral part of a successful new joint venture for Unilever's ice cream business, which included franchise operations. Kevin has also worked in Canada and in the US for a division of Dresser Industries, as a technical marketing representative. Finally, he was a founding member and director of a Canadian biotech startup.

Kevin holds a Bachelor's degree in Chemical Engineering and an MBA in International Business & Marketing.

Kevin Joy
Vice President, Marketing
BD-BrandProtect
Tel: 905.271.3725 ext. 306
kjoy@bdbrandprotect.com

