

Internet threats and the rise of social media

By Michael M. Kiefer, General Manager, BrandProtect

Introduction

You are a target. Your institution is a target.

The rapid adoption of social media is creating serious security challenges for the banking industry. In the near future, it is likely you will need to respond to a social media incident impacting you, your board, your employees, your customers and your loss reserves.

Welcome to the Internet. And welcome to your next headache. Social media threats are an area seemingly beyond your control but well within your regulatory responsibility.

So as a bank officer or director, how should you protect yourself from attacks that target your rights, revenue and reputation but never touch your IT network?

Reports of data compromises and security breaches triggered by social media are in the news almost every day. The ingenuity of Internet criminals continues to surprise and amaze law enforcement.

How should you adapt your existing risk management and incident response framework to accommodate threats such as identity theft, reputation extortion, phishing (email attacks), Vishing (Voice attacks that compromise accounts), SMSHING (Cell phone Text message attacks), YouTube, Twitter, Facebook and a whole host of evolving, new and yet to be named attacks, venues and buzz words that can often times seem overwhelming?

In other words, how should your risk management and incident response framework anticipate what former Secretary of Defense Donald Rumsfeld called the “unknown unknowns?”

There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know.

- Donald Rumsfeld

As you plan for the unknown unknowns of social media, the massive public relations SNAFUs of Domino's Pizza (Employees/conduct/YouTube) and Barclays (Blog posts/pre corporate disclosure) should weigh heavily on your mind.

Not too long ago, Toby Bell, a leading analyst at Gartner Research, published a paper entitled “Policies and Procedures to Manage Enterprise Internet Reputation.”

The Gartner team discussed social sites that can have an impact on corporations and brands. They found that “social media is an unfamiliar territory for enterprises, with very different rules for engagement,” and that “...social media blurs the demarcations between public and private information, increasing the likelihood that consumers will unintentionally or negligently say publicly what they meant to say privately.”

The Net-Net is that bank officers and directors need to understand the risks of these mediums and have a clear plan for monitoring, managing and mitigating threats that can and will occur.

New factors impacting your risk management framework

These threats bulleted below illustrate the type of social media infractions that can occur against your brand on the Internet.

Quick! Who owns these threats? And, how will you respond when they happen?

- Someone is thinking about climbing into your pre-shred dumpster, video taping themselves reading sensitive customer files and releasing the video to YouTube. If you're lucky, it may just be for fun, not extortion.
- A typo squatter has registered domain names that emulate your domain (your-domain-misspelled.com) so they can steal identities via malware downloads, steal money via login scams, steal traffic for monetization or many other nefarious activities.
- A hacker is posing as your IT department to collect passwords and sensitive customer data from your senior managers, tellers and officers.
- A job posting on a job board for EVP in your institution that is an identity theft scam.

The ownership of these threats is not always clear.

Socially networked enterprises risk business disruption, brand damage, and even loss of consumer Personal Identifiable Information (PII).

Since the attacks occur beyond the network perimeter or outside the firewall, IT is only marginally involved. Branding and marketing and public relations are interested but lack the process necessary to manage risk. E-business and human resources are shared services that provide training and development capabilities. Corporate legal, security and fraud don't have the budget. Ops doesn't have the staff. So who is responsible?

No clear ownership of social media risks creates additional risks. Do not assume someone else is paying attention.

The lack of organizational ownership plus the other unknown unknowns of social media leave many shareholders, executives and board members wondering about their risk exposure.

Enter Enterprise Internet Risk Management

Online attacks, identity theft and Internet fraud can never be completely defeated, only mitigated.

As a result, there is now urgency for someone to immediately establish an enterprise-wide state of readiness to combat brand abuse from social media and identify ways to reduce the severity of reputational risk to the corporate brand. Organizations must attest to the effectiveness of their internal processes.

An enterprise-wide approach is necessary to properly manage these rapidly evolving threats.

Enterprise Internet Risk Management (EIRM) eliminates traditional silos where each area of the organization manages risks separately and instead builds capacity using integrated processes, people and technology all working to minimize the damage that can be inflicted on both corporate brands and customer trust.

In adopting EIRM, 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:

- 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.
- 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.
- Corporate training should 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.
- 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.
- 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.

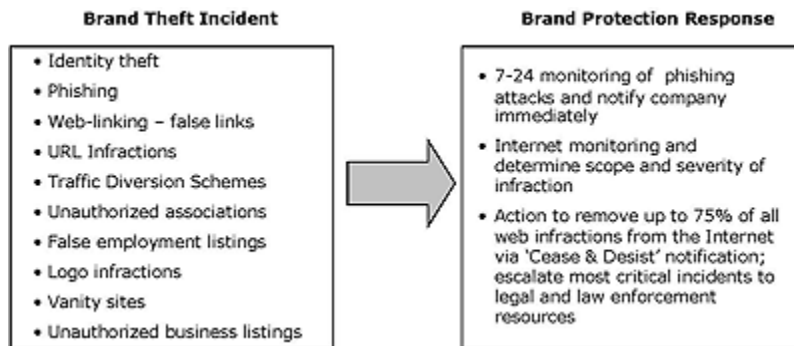


Figure 3 – Collaborative proactive brand protection

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.”¹

To mitigate the negative effects of security breaches, organizations are finding it necessary to develop formal incident response programs (IRPs). However, at a time when organizations need to be most prepared, many banks are finding it challenging to assemble an IRP that not only meets minimum requirements (as prescribed by Federal bank regulators), but also provides for an effective methodology to manage social media security incidents for the benefit of the bank and its customers.

Designing an incident response plan (IRP)

So how do you respond to the unknown unknowns? Your ability to respond to Internet attacks on your brand in a planned and coordinated fashion is critical to the success of your EIRM program.

First, understand that prevention is probably impossible. Every bank is susceptible to the many evolving threats including threats from disgruntled employees and customers.

Formal incident response planning combined with strong internal awareness training will not prevent future incidents but will allow you to rapidly reduce the level of brand damage.

While regulatory agencies mandate certain IRPs be part of your information security program, social media and brand related attacks fall into a grey area outside of Information Security’s responsibility.

Using Federal Bank guidance to incorporate social media brand attacks into IRP is a simple process. Developing a social media or a brand attack IRP is in the bank’s best interest and will make your brand stronger over the long-run.

In many ways an IRP is similar to disaster recovery planning. A solid IRP will anticipate the unknown unknowns and work to patch weak points in the brand perimeter. The need for comprehensive response programs is real and required by the banking industry.

Although preparation may require considerable time and cost, the benefits can be well worth these expenditures.

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

¹ “Secure the Trust of Your Brand: How Security and IT Integrity Influence Corporate Reputation”, A CMO Council Report, September 2006, page 21

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.

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.

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 the Author

Michael M. Kiefer, General Manager, BrandProtect. A recognized network security expert and IT and risk visionary, Mr. Kiefer brings more than 25 years of network, telephony, Internet and disaster recovery experience to his role at BrandProtect, where he is responsible for Global operations. He is also a board member of FS-ISAC. He can be reached by email at mkiefer@brandprotect.com or contacted at 224.766.3000

Published by:
Financial Managers Society, Inc.
100 W. Monroe, Suite 810
Chicago, IL 60603
312-578-1300
info@fmsinc.org
www.fmsinc.org