

WHITEPAPER

**Mitigating the Costs of Threats
Associated With Your
Internet Presence**

Target Audience: Financial Institutions

Authored By:

Kevin Joy, Vice President, Marketing
BD-BrandProtect

June 6, 2007

Table of Contents

Introduction	3
Assessing Your Exposure to Threats on the Internet.....	4
Elements of an Effective Internet Presence Threat Analysis.....	5
Conclusion.....	9
About BD-BrandProtect	10
About the Author.....	10

Introduction

Each year, the risks associated with Internet banking rise. Today, consumer confidence is threatened and customers are increasingly at risk from an expanding range of Internet incidents aimed at financial institutions, such as:

- Phishing attacks, where Internet criminals attempt to dupe customers into releasing their personal financial data in order to commit identity theft
- Weblinking incidents, where customers click on links that appear legitimate, only to be diverted to unrelated and potentially offensive sites
- Brand protection incidents that target an organization's brand and misuse it to claim an unauthorized association, divert Web traffic or commit fraud, and
- Domain incidents, where Internet fraudsters "hijack" Web domains while attempting to find ways to monetize them to their own advantage

These emerging threats are rapidly exposing financial institutions to a range of unprecedented financial, legal, strategic, reputation, operational and transactional risks. This is especially true as agencies across the country continue to indicate stronger intentions in holding financial organizations to a higher standard of responsibility in protecting both the corporation's and its customers' information assets from reasonably foreseeable threats.

From section 501(b) of the *Gramm Leach Bliley Act* and the Interagency Guidelines Establishing Standards for Safeguarding Customer Information to regulations and guidance released by organizations such as the FFIEC (Federal Financial Institutions Examination Council), FDIC (Federal Deposit Insurance Corporation) and NCUA (National Credit Union Association), financial organizations today face spiraling expectations regarding their role in protecting their customers and other stakeholders from Internet threats. The repercussions of failing to comply with these measures can range from fines and sanctions to lost revenue, deteriorating customer loyalty and a loss of brand integrity.

Given the dangers of non-compliance, it is incumbent upon financial institutions to take the necessary steps to assess their exposure to threats on the Internet. This paper outlines some strategies organizations can take to succeed in this effort.

Assessing Your Exposure to Threats on the Internet

As the FFIEC notes in its E-Banking Booklet, no single control or security device can adequately protect a system connected to a public network, such as the Internet. As a result, financial institutions must establish layers of various control, monitoring and testing methods to mitigate the risks associated with maintaining an Internet presence. Some of the controls recommended by the FFIEC include:

- Maintaining an ongoing awareness of attack sources, scenarios and techniques
- Adopting a rapid response process to react to newly discovered threats
- Implementing controls to prevent malicious code
- Adopting rapid intrusion detection and response procedures, and
- Engaging in independent testing, through audits, security assessments, vulnerability scans and penetration tests

Although regulatory guidance does not specifically outline the threats to be assessed as part of an Internet vulnerability scan, BD-BrandProtect has compiled a list of best practices against which industry participants can benchmark the effectiveness of their Internet presence threat analysis. For instance, in identifying potential areas of exposure, financial institutions should understand the probability they face of experiencing significant Internet incidents, such as phishing, weblinking incidents, brand incidents and domain registration incidents. Armed with this knowledge, organizations can examine a range of inputs to assess their exposure to threats on the Internet.

Keep in mind, too, that the FFIEC distinguishes between threats and vulnerabilities. Specifically, threats are events that could cause harm to the confidentiality, integrity or availability of information or information systems. They can be characterized as the potential for agents exploiting a vulnerability to cause harm through the unauthorized disclosure, misuse, alteration or destruction of information or information systems.¹

For their part, vulnerabilities are seen as weaknesses in a system or control gaps that, if exploited, could result in the unauthorized disclosure, misuse, alteration or

¹ FFIEC Information Technology Examination Handbook, Information Security Booklet, found at http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm

destruction of information or information systems. Vulnerabilities are generally grouped into two types: known and expected. Known vulnerabilities are discovered by testing the environment and through knowledge of other weaknesses. Conversely, expected vulnerabilities are those that can reasonably be anticipated to arise in the future. These may include new and unique attack methodologies.²

As Internet threats become more pervasive, it is increasingly likely that regulators will expect financial institutions to screen for a growing number of expected vulnerabilities. To meet the appropriate level of regulatory compliance, then, financial organizations must come to understand the elements of an effective Internet presence threat analysis.

Elements of an Effective Internet Presence Threat Analysis

In conducting an Internet presence threat analysis, it makes sense to begin by defining the scope of the initiative. In this regard, financial institutions should take into account the various laws, regulations and guidelines that apply to this type of assessment. As noted earlier in this paper, when structuring an information security program under GLBA rules, financial institutions should review the risks and threats related to:

- Risk assessments performed to assess controls on customer information systems
- Monitoring systems and procedures used to detect actual and attempted attacks on, or intrusions into, customer information systems, and
- Response programs developed that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems

In conducting this review, financial institutions are given latitude to define the scope of their assessment, based on their specific operating environment, the complexity of their business and the sensitivity of the information to be protected. That said, regulators have provided some guidance on the types of incidents or events that should be reviewed. Specifically, financial institutions are encouraged to review their

² Sic

exposure to certain enumerated risks by conducting various types of assessments, as follows:

Review exposure to:	By assessing:	To:
Financial risk, transaction risk, compliance risk, reputation risk, legal risk	Phishing, pharming and malware threats	<ul style="list-style-type: none"> • Prevent disclosure or theft of confidential customer information • Mitigate against reasonably foreseeable threats • Shut down fraudulent sites • Protect customers' identities
Potential for customer harm	Weblinks across the Internet	<ul style="list-style-type: none"> • Prevent customer confusion • Ensure customers are not exposed to offensive or inappropriate material
Risks to customer information	External and internal security threats	<ul style="list-style-type: none"> • Maintain customer confidence • Prevent a decrease in the rate of return on strategic investments
Financial risk, transaction risk, compliance risk, strategic risk	Domain names	<ul style="list-style-type: none"> • Prevent domain hijacking • Forestall potential phishing attacks • Prevent traffic diversion • Identify "cybersquatting"
Reputation risk	The corporate website	<ul style="list-style-type: none"> • Prevent defacement

As part of their compliance programs, many financial institutions already engage in ongoing assessments of their internal information systems to identify and mitigate against identified risks. However, the rapid growth of the Internet and the constantly evolving nature of e-crime make it particularly difficult for organizations to maintain the internal expertise required to adequately assess external risks that originate over the Internet, such as phishing, weblinking incidents, brand protection incidents and domain registration incidents.

To properly monitor, measure and prioritize their exposure to these Internet threats, then, it makes sense for financial services organizations to turn to third party experts capable of helping them bolster their compliance efforts. As with any type of risk or threat analysis, this process should begin with an information gathering phase, followed by analysis and response prioritization.

Phase I: Information gathering

An effective threat analysis should be based on an understanding of your organization's current operating and business environments. In compiling this background information, look for specialists with experience conducting in-depth document reviews and consultations designed to identify risks on the Internet. In addition to reviewing the internal environment, you should also look for specialists with the technological capacity to monitor all potential incidents, no matter where they're located across the Internet. Using sophisticated filtering and detection processes, bolstered by human analysis, these specialists should be able to help you:

- Identify significant Internet incidents and malicious activities and break down the incidence of these activities by volume and source
- Identify the types of sites where Internet incidents appear to help prioritize responses to each event
- Determine the reach of each incident
- Assess the potential impact of each incident based on its weight or severity by reviewing issues such as the extent of lost revenue, breaches in customer confidence and trust, the value of broken links and the offensiveness of any sites to which customers may be inappropriately directed due to traffic diversion schemes
- Assess the frequency of each incident
- Determine the complexity of each incident's methodology to gauge how difficult it may be to eliminate specific incidents
- Identify the probability of customers being exposed to each incident to help assess its potential impact

Phase II: Analysis

After identifying the full range of Internet presence threats, it is important to assign risk ratings to the various identified incidents. In measuring risk, look for specialists that can help you assess the probability of each incident's occurrence and gauge the potential impact of exposure. By measuring both probability and impact, you can assign high, medium or low risk ratings to each identified incident.

In assigning risk ratings, it is also helpful to establish a boundary of acceptable risk in advance. Using this boundary as a baseline, organizations can more easily identify

threats that require priority response versus those that do not require equivalent levels of mitigation. To help you establish the boundary of risk that best applies to your organization's risk tolerance, it makes sense to work with professionals who can provide you with access to industry best practices and benchmarks. Relying on this background information, financial institutions can more confidently compare or analyze their baselines relative to their peers and competitors.

Finally, no analysis would be complete without a detailed report outlining the results of the assessment process. To help improve your decision-making, ensure the reports you receive present data that is prioritized rather than simply providing raw numbers.

Phase III: Response prioritization

As a final step in your threat analysis, it is essential to prioritize responses to the various identified incidents, based on their risk ratings. While responses will vary depending on your needs and circumstances, consider working with specialists who can help you implement key response measures, such as:

- Removing Internet incidents through takedown services and engaging in ongoing monitoring to ensure targeted sites do not reappear
- Establishing a response team responsible for detecting, responding to and preventing new incidents that emerge over time
- Initiating customer communication campaigns designed to alert customers to potential threats and educate them on strategies for protecting the confidentiality of their information on the Internet
- Alerting national and global authorities in instances of potential criminal activity, and maintaining appropriate records and logs
- Removing inappropriate weblinks
- Monitoring recurring instances of domain registration incidents
- Alerting you to potential brand infringements by your distribution and channel partners

Conclusion

As the threats associated with maintaining an Internet presence continue to proliferate, financial institutions must put proactive strategies into place to respond appropriately. Only through regular threat analysis can organizations hope to counter the risks posed by Internet incidents, which range from financial loss, reputation damage and transactional risks to the potential for inflicting customer harm, which could lead to penalties and fines associated with regulatory non-compliance.

Approached actively, however, Internet presence threat analysis can deliver a range of immediate and long-term benefits by helping financial institutions:

- Benchmark against industry standards
- Increase their understanding of defined risks and better manage them
- Enhance regulatory compliance and corporate governance by monitoring, managing, mitigating and reporting on Internet threats
- Protect their brands from reputation damage and loss
- Reduce the likelihood of negative Internet-based events
- Formulate and execute an Internet compliance strategy to minimize the costs associated with identified incidents
- Recover from a compliance failure or a phishing or domain registration incident

In today's heightened regulatory environment, financial organizations are coming to understand that compliance must be approached holistically, across the entire enterprise. As part of this approach, leading organizations have begun to define their internal assessment capabilities, and carve out responsibilities for external assessments to experienced third party specialists. By combining these review activities, financial institutions can begin to develop sustainable compliance programs designed to help them protect their brands, prevent customer harm and address other potential risks over time. At the same time, they can establish safe and effective strategies for leveraging the significant opportunities offered by the Internet and assuage customers' fears in the process.

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

06/06/07 v 03

