

# The Benefits and Risks of Web 2.0

**An Osterman Research White Paper**

*Published June 2010*

***SPONSORED BY***

**M86™**  
SECURITY



## Why This Document Will Be Worth Your Time

---

- In June 2010, up to 114,000 Web sites, including those of the *Jerusalem Post* and the *Wall Street Journal*, were infected with software that attempts to install malware on visitors' computers<sup>1</sup>.
- Also in June 2010, a new attack directed against Facebook prompts users to click on a post which some of their friends have supposedly "liked". Clicking on a post resulted in a new post to the infected user's Facebook wall<sup>2</sup>.
- Malicious code can exploit an ActiveX vulnerability in versions of Skype's EasyBits Extras Manager dated prior to October 12, 2009<sup>3</sup>.
- Posted on Twitter in June 2010: "Hate that one client we have!! The workflow is a mess and they're so stupid! And impolite."

### KEY TAKEAWAYS

The Web, Web 2.0 applications and social networking tools are incredibly useful: they can make employees more productive and speed decision-making, they can allow companies to gain a competitive advantage over their rivals, and they can significantly reduce the cost of doing business.

However, these capabilities also represent an enormous risk. Web-based malware, for example, which accounts for more than 90% of the malware sent across the Internet, can result in enormous financial losses by draining bank accounts or accessing login credentials for sensitive corporate data stores. Users can employ these tools to inadvertently share trade secrets or embarrassing information. Web-based tools can result in the compromise of corporate security defenses, allowing hackers into any part of a network.

Further compounding the problem is that Web security gateways and other defenses are not deployed as widely as they should be; corporate security policies are mostly either lacking in specificity, they are not enforced or they are non-existent; and users are not sufficiently educated about the Web-focused policies that do exist.

### ABOUT THIS WHITE PAPER

This white paper focuses on both the benefits and risks associated with the use of the Web, Web 2.0 applications and social networking tools. It discusses the recommendations for improving an organization's security posture with regard to use of these tools, and it provides an overview of M86 Security, the sponsor of this white paper.

---

<sup>1</sup> <http://is.gd/cRLey>

<sup>2</sup> <http://is.gd/cRLbt>

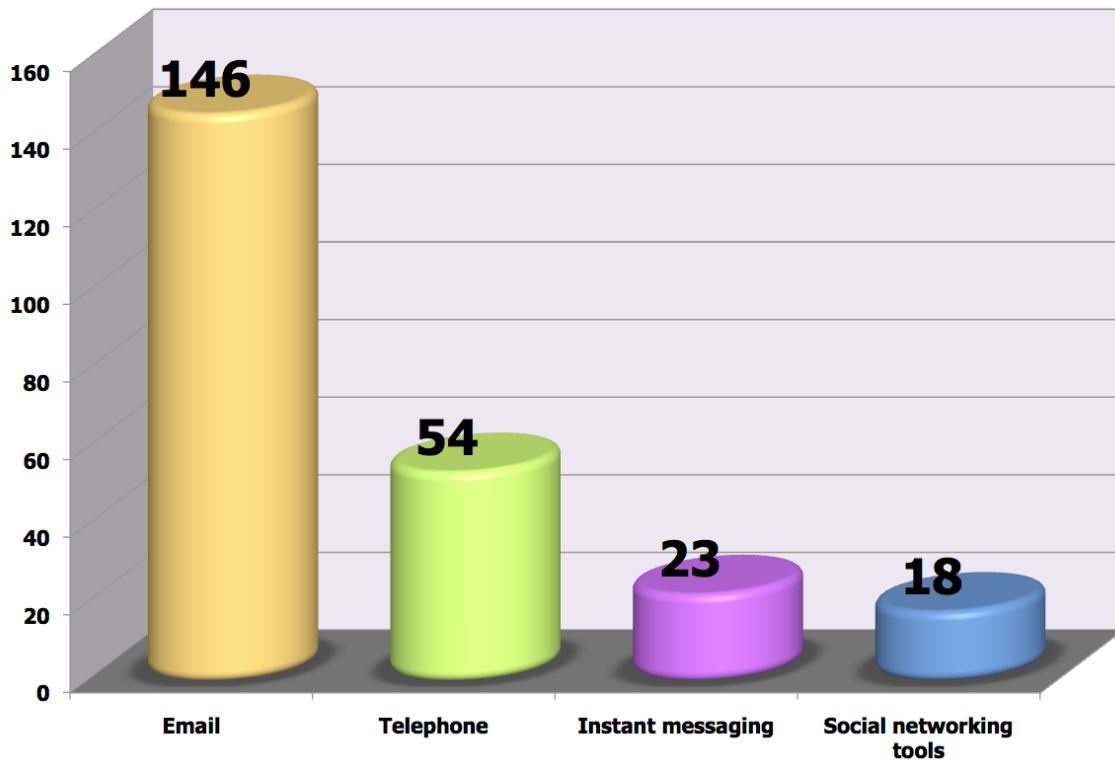
<sup>3</sup> <http://is.gd/cRLhB>

## The Benefits of the Web and Web 2.0 Applications

### EMAIL STILL DOMINATES CORPORATE COMMUNICATIONS, BUT...

An Osterman Research survey conducted during May 2010<sup>4</sup> found that the typical email user spends nearly 2.5 hours per day working in email, far more than other communications medium, as shown in the following figure.

Minutes Per Day Spent Using Various Communications Tools



Another Osterman Research survey conducted in March 2010<sup>5</sup> found that the typical user sends and receives 160 to 173 emails on a typical workday (depending on the size of the company), resulting in the sending or receipt of an email every three minutes or less during a normal workday. Clearly, email is still the dominant communication medium for the typical user.

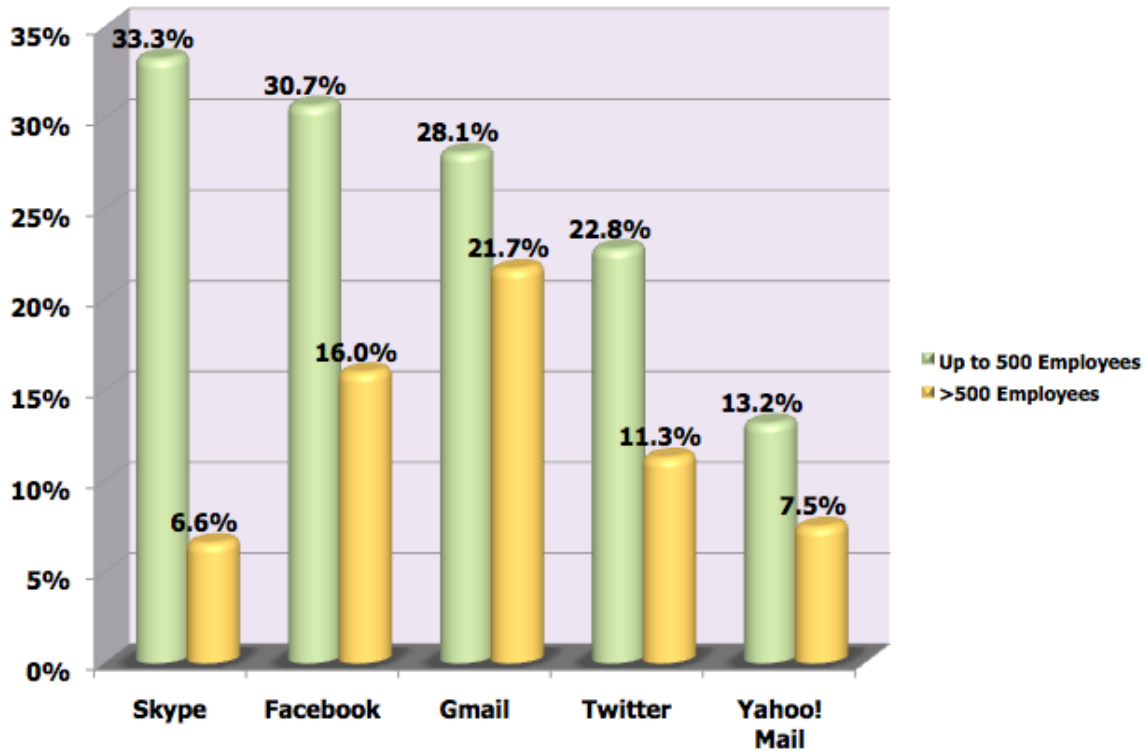
### ...THE WEB AND WEB 2.0 ARE FINDING INCREASED POPULARITY

Despite the dominance of email for communications, the Web and various Web 2.0 applications are finding increased use for a wide variety of applications. For example, the March 2010 survey referenced above discovered that Web 2.0 tools are fairly widely used in both small and large organizations, as shown in the following figure.

<sup>4</sup> *Messaging Policy Market Trends, 2009-2012*; Osterman Research, Inc.

<sup>5</sup> *Results of a Survey on End User and IT Messaging Issues*; Osterman Research, Inc.

Use of Various Web 2.0 Tools



Further, industry data shows that users are increasingly employing the Web and Web 2.0 tools. For example:

- In April 2010, 110 billion minutes were spent on blog and social networking sites – the typical visitor spent two-thirds more time on these sites compared to a year earlier<sup>6</sup>.
- In April 2010, blog and social networking sites attracted 24% more online users compared to a year earlier<sup>7</sup>.
- There are currently 190 million users of Twitter<sup>8</sup>, 519 million users on Facebook<sup>9</sup>, 65 million users on LinkedIn<sup>10</sup> and 115 million on Friendster<sup>11</sup>.

**MANY USE THE WEB AND WEB 2.0 FOR REAL-WORLD APPLICATIONS**

Although social networking tools have a reputation in the popular press for trivial applications, such as informing the world of what tweeters or posters had for breakfast, there are a growing number of useful applications for social networking and related tools. For example, some rely on these tools for receiving breaking news from trusted

<sup>6</sup> Source: The Nielsen Company, April 2010 (<http://is.gd/cR9GP>)

<sup>7</sup> Source: The Nielsen Company, April 2010 (<http://is.gd/cR9GP>)

<sup>8</sup> <http://is.gd/cRaJQ>

<sup>9</sup> <http://is.gd/cRaUd>

<sup>10</sup> <http://is.gd/cRaYw>

<sup>11</sup> <http://is.gd/cRaYw>

colleagues, demonstrating subject-matter expertise to clients and prospects, sending marketing messages, or announcing upcoming Webinars and trade show attendance. These tools can make employees more productive by giving them faster access to information, they can speed decision-making, and they can offer companies a distinct competitive advantage.

In short, social networking isn't just about breakfast anymore!

## **The Risks of the Web and Web 2.0 Applications**

---

### **MOST DECISION MAKERS ARE NOT AWARE OF THE DANGERS**

While social networking and other tools are quite useful and are becoming more so, they also represent a significant threat vector that many decision makers may have not considered as part of their overall security posture. For example:

- Inadvertent data breaches can (and do) occur when users employ Web 2.0 tools. For example, a user can divulge sensitive information or make a comment that can harm the reputation of his or her employer. Among the most egregious examples of this kind of inadvertent mistake was the March 2010 Facebook post by a soldier in the Israeli Defense Forces (IDF) about an upcoming raid that had to be cancelled as a result<sup>12</sup>.
- Malicious distribution of sensitive and confidential information can also occur. For example, in July 2008, an employee with the California Department of Consumer Affairs emailed a file with the names and Social Security numbers of more than 5,000 staff members to her personal Yahoo! account – on her last day of employment<sup>13</sup>.

In addition to human error or malice in the context of data breaches using the Web and Web 2.0 tools, there are a growing number of Web-based and Web 2.0-specific threats. For example, the majority of malware is today distributed through Web sites, not email as was the case just a couple of years ago. One source estimates that a large organization with 40,000 computer users will view 48 million Web pages on a typical day and 0.17%, or 83,000, of those pages will be infected with malware<sup>14</sup>, an average of more than two infected Web pages per user each day.

Although organizations of any size can be impacted by Web-based threats, smaller organizations are particularly vulnerable to Web exploits because they often lack the IT staff and technical expertise necessary to detect and remediate these threats before they can do real damage. Examples of organizations that have been impacted include an auto parts supplier in Georgia that lost \$75,000 to a banking Trojan and a county government in Kentucky that lost more than \$400,000 to a similar exploit.

---

<sup>12</sup> <http://www.allheadlinenews.com/articles/7018132756>

<sup>13</sup> <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

<sup>14</sup> Infected "Legitimate" Site A Growing Threat, *Processor*, October 23, 2009

## **MOST ORGANIZATIONS DO NOT MAINTAIN ADEQUATE DEFENSES**

The majority of organizations either do not maintain adequate defenses against Web-focused threats, or they do not maintain any defenses whatsoever, leaving the organizations exposed to any number of threats. For example, in a survey conducted by Osterman Research in May 2010<sup>15</sup>, 62% of mid-sized and large organizations in North America reported having been infiltrated by Web-based malware during the previous 12 months as a result of simple Web surfing; this compares to *only* 43% of organizations in which malware has penetrated through email. Other problems include:

- Malware has entered 12% of organizations through a Web 2.0 application.
- Sensitive or confidential information was leaked through a social network in 9% of organizations.
- Sensitive or confidential information was leaked through instant messaging in 5% of organizations.

Malware infiltration levels that are this high among mid-sized and large organizations clearly indicate that defenses are definitely not what they should be. Given the quality of Web security gateways currently available, defenses that have been deployed are nowhere near what they could be. This will be an even more serious problem in the future – Osterman Research anticipates that at least 20% of organizations will be the victim of Web 2.0-related malware infiltration during the next 12 months.

## **WHAT COULD GO WRONG?**

There are a variety of quite negative consequences that can arise from data breaches, inappropriate comments and other uses of the Web, Web 2.0 applications and social networking tools. For example:

- **Direct attacks**

Direct hacker attacks can include a variety of exploits, including hackers attacking a known vulnerability in a Web browser, or exploiting an older version of a browser or ActiveX control.

The Secure Enterprise 2.0 forum<sup>16</sup> found that hackers exploit a large number of Web site and Web 2.0 vulnerabilities, including SQL injection as the most common exploit (21% of vulnerabilities), insufficient authentication (18%), content spoofing (11%) and cross-site scripting (11%), among other exploits. WhiteHat Security, in a report published in December 2008, found that 65% of Web sites were vulnerable to cross-site scripting attacks<sup>17</sup>.

- **Blended threats**

Blended threats are an increasingly common threat vector in which spam contains a link to a malicious Web site. Users will often click on a link in a spam message and get infected from the malware-laden Web site that opens in their browser.

---

<sup>15</sup> *Messaging and Web Security Market Trends, 2010-2013*; Osterman Research, Inc.

<sup>16</sup> *Web 2.0 Hacking Incidents and Trends, 2009 Q1*

<sup>17</sup> *WhiteHat Website Security Statistic Report*, Spring 2009, 7<sup>th</sup> Edition

Blended threats are the initial phase of a “drive-by” download that occurs when a user visits a Web site and has malware automatically downloaded to his or her computer. In some cases, a user will visit a Web site and see a popup window – upon clicking the “OK” button in the popup, a Java applet, an ActiveX control, etc. will be installed on the user’s computer without their consent.

- **Cross Site Request Forgery (CSRF) attacks**

In CSRF attacks, innocent-looking Web sites generate requests to different sites. CSRF attacks have exploited vulnerabilities in Twitter, enabling site owners to acquire the Twitter profiles of their visitors.

- **Inappropriate comments that could lead to loss of business**

In January 2009, an employee of public relations firm Ketchum used Twitter to post some very unflattering comments about the city of Memphis shortly before presenting to the worldwide communications group at FedEx – Memphis’ largest employer. An employee of FedEx discovered the tweet, responded to the tweeter, and then copied FedEx’s senior managers, the management of FedEx’s communication department and the powers that be at Ketchum<sup>18</sup>.

A senior manager at FedEx responded to this post with the following: “...everyone participating in today’s event, including those in the auditorium with you this morning, just received their first paycheck of 2009 containing a 5% pay cut...many of my peers and I question the expense of paying Ketchum to produce the video open for today’s event; work that could have been achieved by internal, award-winning professionals with decades of experience in television production.”

It is important to note that social media policies must be enforced particularly for a company’s brand identity and image. Attempting to recover from damage to a corporate brand can be very difficult, a press nightmare and can be quite costly – assuming, of course, that the brand can ultimately be recovered.

- **Violation of the law**

Web-based data breaches and the like could put an organization in violation of their regulatory obligations to protect data, including the Payment Card Industry Data Security Standard, Gramm-Leach-Bliley Act, Health Insurance Portability and Accountability Act, various state breach notification and encryption laws, the UK Data Protection Act, Canada’s Personal Information Protection and Electronic Documents Act and many other requirements.

- **Significant financial loss**

Malware that enters through the Web could install a keystroke logger, for example, on a senior manager’s PC, resulting in the loss of hundreds of thousands dollars in funds from financial accounts. This type of malware is designed to operate quietly and can drain funds for weeks before it is detected.

---

<sup>18</sup> <http://shankman.com/be-careful-what-you-post/>

## **What Can You Do to Protect Your Organization?**

---

### **UNDERSTAND THE NATURE OF THE RISKS YOU FACE**

The first step in protecting any organization from the variety of Web, Web 2.0 and social networking threats it faces is to understand the nature of these threats. There are a variety of sources available to provide this education, including vendors of Web security gateways, industry analysts, consultants, speakers at trade shows, Webinars, the trade press and peers that one might meet at conferences and similar venues. The key for any IT or business manager is to educate himself or herself about the nature of the threats, how they could specifically impact their organization, and the remedies that are available to prevent and/or remediate them.

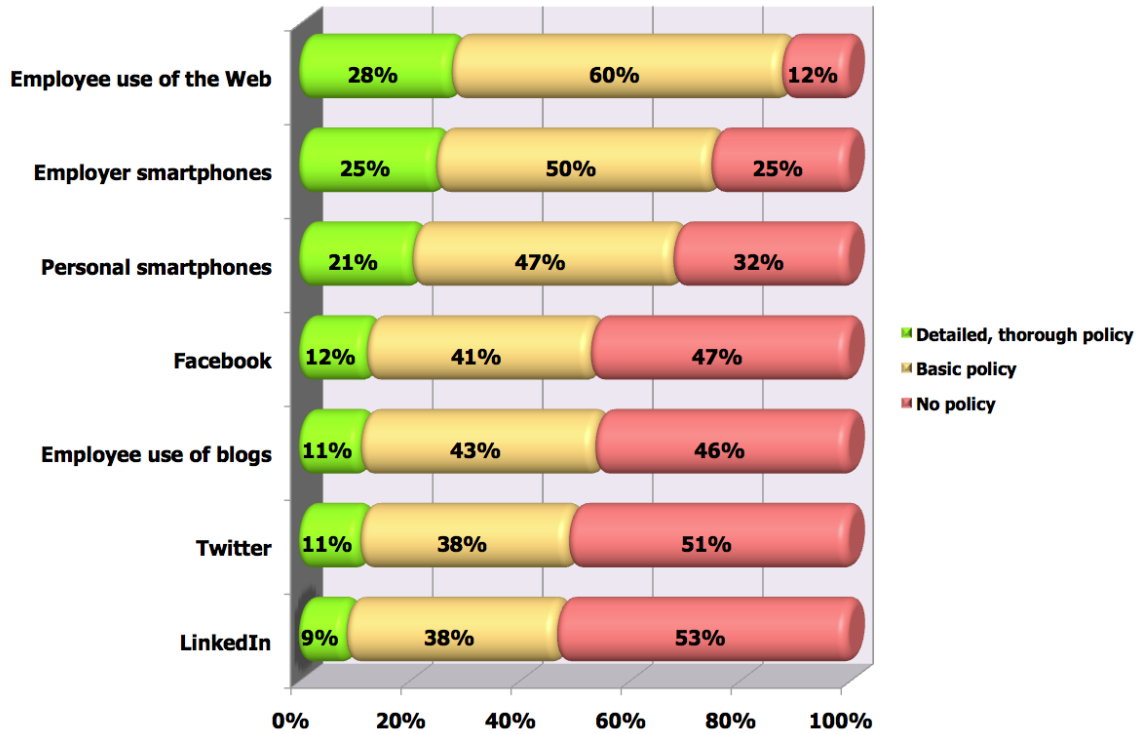
### **AUDIT YOUR WEB SECURITY CONTROLS**

The next step is to carry out a thorough audit of the organization's Web security controls. The goal is to identify the holes in the security systems, including ports that are unprotected, application protocols that are unmonitored, where there are out-of-date or inadequate policies, which policies are enforced and which are not, and the like. The result of this audit should be a vulnerability assessment that clearly defines where the network is protected and where it is vulnerable to attack.

### **ESTABLISH DETAILED CORPORATE POLICIES**

Next, organizations should established detailed and thorough policies about all of the Web, Web 2.0 and social networking tools currently in use or that might be used in the future. Osterman Research has found that the vast majority of organizations have either no policy in place regarding the use of these tools or the policies that exist are fairly basic, as shown in the following figure.

**Current Organizational Policies for Various Communication Tools**



The policies that an organization might want to establish will vary based on the industry(ies) in which they operate, their size, the geographies in which they operate and other factors. However, they should include the tools that can and cannot be used, any limitations on the use of approved tools (e.g., limiting file transfers in some tools), and what is considered appropriate and inappropriate use. A key consideration for decision makers as they create these policies is to move beyond a “block or allow” mentality, instead focusing on *how* tools will be used, not *whether or not* they will be permitted.

**TRAIN EMPLOYEES**

A key component is any security posture, and one for which no amount of technology can compensate, is employee training. For example, in the messaging policy study cited earlier, Osterman Research found that mid-sized and large organizations in North America are slightly more dependent on employee training than they are on technology solutions to ensure messaging-related policy compliance. Although technology is considered to be more effective than employee training at ensuring policy compliance (52% of IT decision makers consider technology to be effective or very effective versus 29% for employee training), employee training is an integral component in ensuring that policies are followed and enforced.

## **DEPLOY ROBUST TECHNOLOGIES**

Finally, organizations must deploy the right technologies to protect against both inadvertent and intentional data breaches. This includes robust Web security gateways that will monitor all of the ports in the network and all of the application protocols that might be in use, as well as the malware that could enter an organization from the Web, social networking tools, Web 2.0 applications and email.

## **About M86 Security**

---

M86 Security is the leading provider of real-time malware protection and largest provider of Secure Web Gateways in the world. Solutions include on-Premises appliances and hybrid cloud solutions.

### **SECURE WEB GATEWAY TECHNOLOGY**

The complete family of M86 Secure Web Gateway products provide large enterprises and medium-sized organizations with a unified Web security solution, which enables productivity, compliance, liability and bandwidth control as well as multi-layered Web security. The M86 Secure Web Gateway delivers:

- **Web security**  
Patented, real-time code analysis engine and optional anti-virus modules.
- **Productivity, liability and bandwidth control**  
URL filtering, content caching and application control technologies.
- **Data Leakage Prevention (DLP)**  
Inspection of outbound communications for sensitive/confidential data, even when hiding in HTTPS/SSL.
- **Flexible central management**  
Central management from the same Web-based console (including monitoring and controlling HTTP, FTP and SSL traffic).
- **Powerful logging and reporting**  
Clear visibility into the entire organization's Web traffic.
- **Integrated mobile and branch office web security**  
Cloud based services provide a hybrid, integrated solution to protect on premise, branch office, and mobile laptop users.

### **PROTECTION AGAINST WEB 2.0 THREATS**

M86 Security's Secure Web Gateway enables users to benefit from the latest Web 2.0 technologies and applications in a secure environment. Organizations can secure and control the way employees use Web 2.0 applications, without the need to completely block them. Collaborative applications such as IM, Skype, and P2P can also be controlled and restricted to uses beneficial to the organization.

Using M86 Web security solutions, organizations can enforce specific policies that suit their organizational needs, such as allowing employees to access Facebook, while preventing them from posting comments or attachments, eliminating the risk of sensitive or confidential data leakage. Policies for each worker remain the same, regardless of location.

M86 Security's Secure Web Gateway is uniquely capable of protecting organizations and companies — regardless of size, location or business activities - against crimeware and malware posted on Web 2.0 sites. Patented, active, real-time content analysis detects malicious code embedded in Web 2.0 pages, and then disables the malware, allowing access to legitimate content on the same page.

M86 Security provides clients with integrated Web and e-mail threat protection, including the most sophisticated Secure Web Gateway available. Our solutions protect organizations and institutions from inappropriate content, legal liability, compromised data, lost bandwidth and reduced network performance. Our e-mail and Web security products monitor and filter malware, spam, non-essential Web applications, distributed content and the many distractions associated with Web and e-mail access—whether they are part of inbound or outbound traffic. These capabilities contribute significantly to the enforcement of Acceptable Use Policies (AUPs), oversight and compliance with regulatory mandates, and maintenance of safe work/learning environments.

### **THE BENEFITS OF USING M86 SECURITY**

M86 Security's customers benefit from our proven Web and e-mail security technology, which correlates real-time intelligence to protect organizations from current and emerging threats. Some—like blended threats—are detected on-the-fly, in real time, via our patented behavioral analysis and content inspection technologies. M86 Security Labs is a specialized team of experts focused on detecting current and emerging threats, and mitigating them by distributing intelligence to the installed base of M86 Web and e-mail security products, worldwide.

Our security labs utilize both data feeds pulled from the Internet security community and internal intelligence gathered from our global deployment of products. Combined, this breadth of threat information provides comprehensive and constantly adapting defense against risks associated with Web and e-mail.

## ***The Benefits and Risks of Web 2.0***

© 2010 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.