Securing Web 2.0 and Social Networking for Enterprise IT

Web 2.0 and social networking technologies have made interactivity a reality—and transformed how the web is used. They also have forever changed the security landscape for both individual users and enterprises. Following is an overview of some common Web 2.0 threats and challenges, and solutions for addressing them.

Malware, security threats, and scams

Users of social networks assume the people with whom they are connected can be trusted. If a “friend” in one’s network posts a URL to a news story, other friends assume it is safe to click the link. They do not exercise the same degree of caution that they might if the link or message was sent via email from a stranger. This lack of discretion can compromise enterprise security: Workers can unwittingly spread malware through corporate networks during the time they spend on social networks.

One popular technique employed by cybercriminals is to lure users into “liking” a particular Facebook page, claiming that the user will see a shocking photo or read a dramatic news story. Once the user has clicked on Facebook’s “Like” button for that page, the page creator can email the user to click other links (that perhaps lead to malware) and can also view the user’s personal information.[1] “Likejacking” increased significantly during the first quarter of 2011, from 0.54 percent of all web malware encounters in January 2011 to 6 percent in March 2011.[2]

Another tactic is to send out fake friend requests, which frequently include a picture of an attractive person. If the recipient decides to view this supposed person’s Facebook page, they will usually find only a single post, which links to some type of scam.[3]

While Cisco’s security experts predict that launching exploits via social networks will become less popular with sophisticated cybercriminals over time[4]—primarily because these efforts can be so resource-intensive—the massive popularity of social networking means the probability of campaigns being launched against users through these channels will remain significant. Thus, businesses still need to take into consideration the risks they could face when workers have unlimited access to social networking tools.

Compliance and data loss

It has never been easier to lose control of corporate data. Information can no longer be locked down within a network—today, webmail, instant messaging, and social networks all offer ways for workers to communicate with people outside the business. This risk is amplified by the increase in remote and mobile workers who need access to data outside of the secure network.

Unfortunately, this makes it easy for users to disseminate information that should not be seen by company outsiders—for instance, attaching documents to Facebook messages or tweeting on Twitter about sensitive

[1] *Cisco 2010 Annual Security Report:* http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf.
[2] *Cisco 1Q11 Global Threat Report*: http://www.cisco.com/web/about/security/intelligence/reports/cisco_global_threat_report_1Q2011.pdf.
[3] Ibid.
[4] *Cisco 2011 Annual Security Report:* http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2011.pdf.

corporate developments. Financial services employees may post information about future earnings releases. High-tech employees might speculate on potential acquisition targets.

Once this information reaches the web, it cannot be recalled like an email message. After someone reads the information, forwards it, and reposts it, it will exist forever on the Internet.

The informality of social networking sites also can seduce users into being considerably less careful about sharing opinions than they would be in conversation or even in other electronic mediums such as email. Information confidential to the employer can easily make its way out into the public domain via the social networking medium. It’s also easy to make a throwaway derogatory comment about an employee, colleague, or customer—and all too easy for that comment to be viewed by a much larger audience than the poster may have had in mind.

The implications of this for the employer are many. At one end of the scale, an organization may suffer financial losses due to brand damage and loss of credibility. Furthermore, organizations that experience Web-2.0-related data may not remain in compliance with government or industry regulations relating to effective systems and processes for data control. This may result in a substantial fine from the regulatory body for failure to manage confidential data with sufficient control or diligence.

Perhaps the worst-case scenario is that of legal action being taken against the organization. In some instances where workers have made indiscreet comments about their organizations via social networks, this has led to lawsuits over harassment, defamation, privacy violations, and ownership of content. Wrongful termination suits related to social media “misuse” also are becoming increasingly common. In fact, the National Labor Relations Board has weighed in on several cases involving employee use of social media and employers’ social media policies—ruling in the employees’ favor in several cases.[5]

Productivity preservation

Another legitimate business concern: Web 2.0 and social networking technology have the potential to undermine business productivity. (Although it should be said that many employers are now turning to social media technology for just the opposite reason: to engage workers and measure their productivity.)

Social networks offer many engaging ways for users to interact, such as games and quizzes, which can draw workers’ attention away from their jobs. Since Facebook opened itself to applications from third-party developers a few years ago, hundreds of thousands of apps have been developed—and have quickly become part of our popular culture. (Zynga’s “Words With Friends” and “Farmville” apps are just two examples.) More than 20 million apps are installed by Facebook users every day.[6]

The challenge for companies is to find a way to preserve workforce productivity by limiting access to social applications without restricting workers’ access to the business benefits that social networking can provide.

[5] “Acting General Counsel releases report on social media cases,” media release, National Labor Relations Board’s Office of Public Affairs, August 18, 2011: https://www.nlrb.gov/news/acting-general-counsel-releases-report-social-media-cases.

[6] “Facebook Statistics, Stats and Facts for 2011,” *Digital Buzz Blog*, January 18, 2011: http://www.digitalbuzzblog.com/facebook-statistics-stats-facts-2011/.

Responding to Web 2.0 Threats with Web Usage Controls

Changing attitudes about where and how work gets done, and the potential productivity benefits of social media, are making it increasingly difficult for organizations to maintain an “all or nothing” stance toward controlling employees’ social network access. Social networking sites have become a hub for many activities, whether people are at work or off the clock. Users can connect with friends and colleagues, share event calendars, promote company news, answer questions from customers, and much more.

This willingness to connect and do business via social networks is only growing as people spend more time doing work outside of the confines of the traditional office environment and the corporate network. In fact, Cisco’s 2011 *Connected World Technology Report* study found that young workers and college students around the globe lean toward the perception that it is unnecessary to come to an office every day for work (although they also recognize that their employers may feel differently).

It is clear that traditional web usage controls can no longer help enterprises effectively manage security, productivity, and data loss and compliance concerns. Attempting to enforce even well-designed acceptable use policies with URL filtering alone is not only a dated approach, but also an ineffective one. While URL filtering is still considered a good first step to mitigating risks posed by social networking sites, it is not a complete solution. And category-based filtering alone will not prevent users from becoming infected with malware.

Real-time scanning, in which all content on a URL is scanned immediately—every time it is requested—is more effective because today’s websites are much more dynamic. A single visit to a single webpage can result in content being delivered from multiple domains across the globe. In addition, social networking applications are far from monolithic. They can be comprised of hundreds of micro-applications—some with legitimate business uses, and others that can be significant drains on productivity. As a result, businesses need social media controls to enable access to some components of an application while blocking others. Since various organizations throughout a company will have different needs, the ability to vary these access rules by functional role is essential.

Solutions that have the ability to identify web content and applications dynamically and apply appropriate policy, even for applications embedded within a website, are more logical and realistic approaches to security challenges in a Web 2.0 world. Following are the types of controls that can effectively enforce security policy, help improve productivity and compliance, and reduce the risk of malware infections and other types of security threats.

Web application visibility and controls

To ensure acceptable use and security policies are enforced within Web 2.0 websites that contain embedded applications, an effective security solution must be able to identify and control, with precision, individual applications utilizing application signatures or other methods. Granular control is critical, considering the volume of actions that can be performed within Facebook—for example, posting content, “liking” a user’s status, sending mail, and chatting. Micro-applications that are used within a bigger application, such as FarmVille on Facebook, also must be identified and taken into consideration by enterprise IT when making access control decisions. To keep pace with changes on the web and ensure effective security and control, signatures also should be updated dynamically.

Dynamic web usage controls

The rise of dynamic webpage generation (pages served up via databases), user-generated content, and password-protected webpages, as well as the popularity of social networking, have led to the creation of billions of pages of web content. By 2015, approximately 95 percent of the websites on the Internet will be uncategorized by

URL filtering lists. This has led to the need for a different approach to applying web usage controls: conducting content analysis of previously unknown sites in real time.

Encrypted web traffic controls

To control data entering or leaving an enterprise network, it is imperative that any solution be able to decrypt SSL packets. Without support for SSL decryption, an IT organization leaves itself open to a large "blind spot," where defined policies are not enforceable.

An effective web security solution should allow security managers to define granular controls over this type of functionality. For example, personal banking sites should be exempt from decryption. However, a phishing site disguised to look like a legitimate personal banking site should be decrypted immediately.

User-based web usage controls

Enterprises should use Internet filtering policies that provide control at the user or group level. This is most successful when a vendor is able to seamlessly integrate with authentication directories such as Microsoft Active Directory.

Time-of-day-based web usage controls

Internet filtering solutions also should be able to accommodate time-of-day-based policies. For example, an organization's security policy may allow for casual use of social networking sites after regular business hours.

Dynamic malware protection

Traditional proxy and web filtering solutions are inadequate protection against web-based malware exploits. Effective protection needs to combine proactive web reputation scoring technology with scanning of content for malware, viruses, and spyware using multiple signature sets from different providers—without impacting the user experience.

Per-object security filtering

A characteristic of Web 2.0 sites is that they contain many objects coming from many different sources. For instance, the popular blog BoingBoing.net has more than 162 different HTTP objects originating from over 30 different domains. In this type of environment, hackers have exponentially more entryways from which to launch exploits.

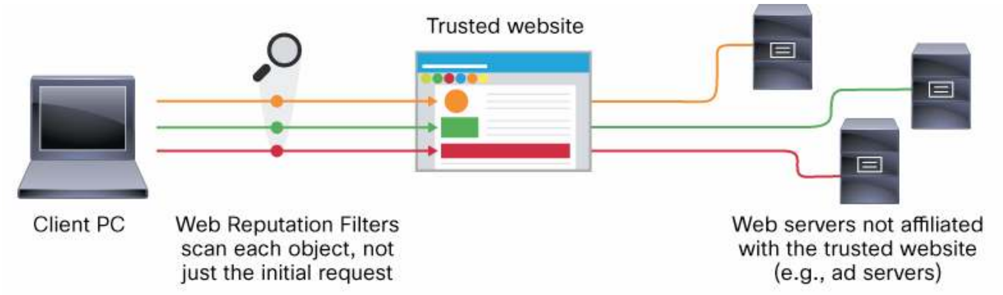
As an example, an international crime ring was behind a recent scam that resulted in compromised users losing more than US$2 million. Cybercriminals created a fake ad agency and submitted an ad for a hotel chain on a Minneapolis newspaper's website. Once the ad was posted, they changed the ad's computer code so users who clicked on it were infected with malware.[7]

To protect enterprises from this type of threat, a gateway vendor can block the entire website until the malware has been removed by the site's webmaster. But if the website is useful for the business, blocking access will only lead to multiple help-desk calls and more work for the IT department.

A second approach is to filter websites on a "per-object" basis (Figure 1). In this approach, only the malware on a website will be blocked. On a blog with a fake ad, for example, only the malicious ad is blocked. This approach requires an underlying vendor solution that is based on a proxy architecture.

[7] "FBI Busts International 'Scareware' Rings," by Chloe Albanesius, PCMag.com, June 23, 2011: http://www.pcmag.com/article2/0,2817,2387467,00.asp.

Figure 1. Per-object security filtering with Cisco Web Security


Trusted website
Client PC
Web Reputation Filters scan each object, not just the initial request
Web servers not affiliated with the trusted website (e.g., ad servers)

Data leakage controls

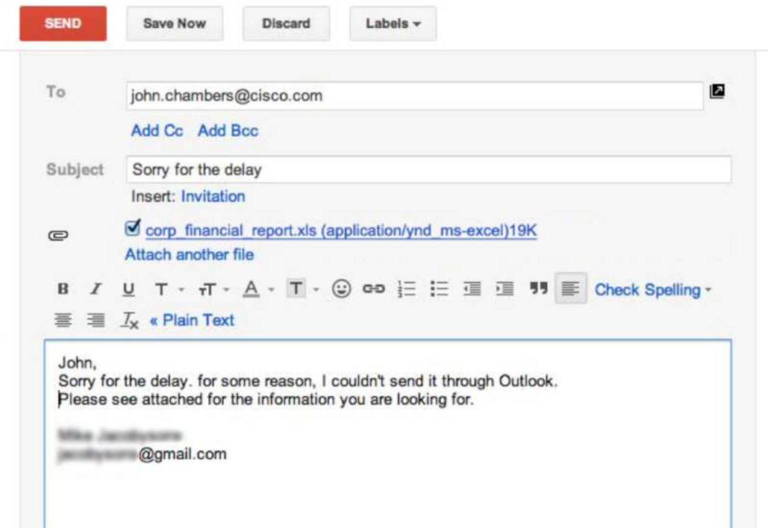
As the web has become a venue for bidirectional communication, control over web content also must be bidirectional. Policies and content analysis must take into account all information leaving the organization to prevent sensitive data from leaking.

In general, enterprise IT departments have dedicated substantial resources to securing outbound messaging through traditional corporate systems such as Lotus Notes and Microsoft Exchange. However, organizations that do allow access to webmail services such as Gmail or Hotmail need additional security controls.

End users who have access to webmail sites can potentially create additional gaps through which sensitive information can leave the organization. For instance, workers might use webmail to communicate with customers or vendors if there is a problem with the corporate email system. Or, they might use webmail to funnel sensitive information out of the company to a competitor.

Web security vendors should provide a way to enable this type of communication without outright blocking of webmail services (Figure 2).

Figure 2. A typical webmail service



To: john.chambers@cisco.com

Subject: Sorry for the delay

☑ corp_financial_report.xls (application/ynd_ms-excel)19K

John,
Sorry for the delay. for some reason, I couldn't send it through Outlook.
Please see attached for the information you are looking for.

[redacted]
[redacted]@gmail.com

Cisco Solutions

Traditional web usage controls can no longer help enterprises effectively manage security, productivity, and data loss and compliance concerns. Today's organizations need solutions that will allow workers to have anytime, anywhere access to the Web 2.0 services they need, while protecting the enterprise from the security threats these channels can present. Smart solutions offer dynamic content controls that can safely enable Web 2.0 within the enterprise while setting appropriate security limits.

Security in the modern network also requires visibility and control beyond the traditional IP- and port-based approach. The proliferation of web-based applications and the port- and protocol-hopping nature of Web 2.0 applications like Skype means ports and protocols are no longer good proxies for applications. "Next-generation" firewalls address this issue by offering application-based visibility and control. However, merely classifying an application is not enough—as discussed earlier in this paper, micro-applications also need to be considered when applying and enforcing security policy. In addition, there is so much more going on in the typical network today that application and user awareness alone are insufficient to assist administrators with actionable security enforcement.

Because there is no one-size-fits-all approach to security—and because how and why an organization uses Web 2.0 tools and technologies depends on its unique business needs, structure, workforce, and culture—enterprises need to have choices. Cisco offers a number of innovative solutions, on-premise and cloud-based, that are designed to provide enterprise IT with application visibility and control for securing Web 2.0 and social networking.

To learn more about Cisco security solutions, go to www.cisco.com/go/websecurity.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-704647-01 12/12