Top Ten Web Threats

And How to Eliminate Them

Symantec.cloud

White Paper: Web Security

Top Ten Web Threats

And How to Eliminate Them

Contents

Introduction: Top Ten Web Threats

The worldwide web is a fantastic business resource but, without proper protection and management, it is also a source of danger and unnecessary expense for small and medium-sized businesses. Based on a survey of 273 IT managers, we reveal the top ten web threats to business and outline a solution that uses Security Safeguard.cloud.

The internet future has arrived. In the US, 61 percent of households have internet access and access the internet almost every day[1]. A current FIND/SVP American Internet User Survey estimates that there are 27.7 million adult Internet users who currently use one other Internet application besides e-mail[2]. It's the same at work. Nearly all American companies have a connection to the internet and employees expect to have internet access at work just like they do at home.

Business Challenges

Allowing employees internet access raises real challenges for IT managers who have to protect the business against malware, keep internet bandwidth available for legitimate business needs and enforce acceptable use policies for the HR department. Managers everywhere must also find a balance between allowing reasonable personal internet use at work and maintaining productivity and concentration in the office.

Web threats fall into two main categories. First there are the things that employees do online – like visiting infected websites. Then there are the challenges and difficulties facing IT managers when it comes to managing web use in a secure and efficient way.

The Top Ten Issues

We surveyed 273 IT managers to find out what kept them awake at night and what challenges they faced. The top ten issues were:

1. Time-wasting on social networking and similar sites (86 percent)
2. Enforcing acceptable use policies (53 percent)
3. The ability to monitor employee web use (52 percent)
4. Keeping security systems up to date with patches and signatures (49 percent)
5. Legal risks such as employees visiting inappropriate websites (44 percent) and the accidental disclosure of confidential information online (57 percent)
6. Keeping internet bandwidth free for legitimate business use (44 percent)
7. Protecting remote and home workers (42 percent)
8. Employees using unauthorised web-based applications (42 percent)
9. Protecting the organization against spyware and malware (40 percent)
10. Protecting multiple offices and locations (19 percent generally but 76 percent among companies with 500 or more employees)

This report looks at each of these concerns to understand the business issues and to propose solutions based on Symantec.cloud.

1-2007 US Census Data, http://www.census.gov
2-http://www.networkworld.com/news/2007/050707-employee-web-use.html

Protecting Your Business

Threat	Why it matters	How to protect your business
Time-wasting online	The Confederation of Business Industry estimates that people spend more than 90 minutes a week on personal websurfing at work[3]. It reports that a third (32 percent) of the companies it surveyed had had to discipline an employee for internet misuse. Endemic time-wasting saps productivity and discourages honest workers who have to pick up the slack. Dealing with the disciplinary issues is a serious drain on management time. It is a big issue for managers in every company. For example, 86 percent of the IT managers we surveyed worried about it.	Only 44 percent of the IT managers we surveyed had the ability to restrict access to non-work websites. Without this kind of technology, employee time-wasting goes unchecked and policy enforcement becomes much more difficult. MessageLabs Security SafeGuard lets you set and apply consistent policies that restrict access to different categories of website. However, many companies take a more permissive approach and accept that a certain amount of personal internet use is acceptable; indeed many prospective employees now see it as a right. So the MessageLabs Security SafeGuard lets you apply time and bandwidth limits on use so that people can have access but within reasonable boundaries.
Enforcing acceptable use policies	Seven in ten of the IT companies we surveyed had an acceptable use policy for the internet. Given the risks, such a policy is essential along with training to educate users about it. But without the technical means to enforce company policies, companies are at greater risk. For example, inconsistent enforcement and rule making on the fly makes disciplinary action harder. Only 57 percent of the people we surveyed could enforce acceptable use policies in a consistent way.	An effective web filtering and monitoring service can help enforce an acceptable use policy. A good system, such as MessageLabs Security SafeGuard, allows a high level of control over what types of sites can be blocked and an extensive database of websites to make sure nothing slips through the cracks.
Monitoring web usage	Only 48 percent of the people we surveyed were able to get detailed reports on web use. However, effective monitoring and reporting has a powerful deterrent effect. It can also help companies with very restrictive policies justify a degree of relaxation; for example, to allow employees access to personal sites during the lunch hour. But without effective reports, companies are just blind.	MessageLabs Security SafeGuard provides detailed reports to give managers insight into employees' web use. This supports HR investigations and gives managers a broad picture of company-wide usage patterns and productivity.

[3]Employee personal websurfing: http://www.cbi.org.uk/ndbs/Press.nsf/0363c1f07c6ca12a8025671c00381cc7/94d596bf6bcd697
08025745e003b722b?OpenDocument

Threat	Why it matters	How to protect your business
Staying up to date with patches and signatures	Nearly half of respondents (49 percent) reported that keeping security systems up to date with security signatures, software patches, etc. was their biggest management challenge. Doing it properly absorbs a lot of time, while doing it poorly exposes IT systems to unnecessary risk. Typically in-house web filters, policy engines, spam and anti-malware systems need regular updates to stay effective. Finding IT technicians with the right level of skill to manage these systems is another aspect of this problem.	An internet-hosted service, such as MessageLabs Security SafeGuard, removes many of the challenges and most of the drudgery of staying up to date. It doesn't replace client-based anti-malware but it protects email servers and provides a layer of security and management to web browsing in place of in-house systems. Symantec.cloud updates the service many times a day to ensure it stays ahead of the latest threats. Unlike signature-based systems, there is no delay while an update is prepared, distributed and installed. It's all done in our data centers automatically.
Legal risks	More than half our respondents worried about employees visiting inappropriate or offensive websites. Businesses face serious legal liabilities from employee's misuse of the internet: for example, if they download pirated software it can leave directors personally liable. Similarly, downloaded porn can create a hostile environment for co-workers and grounds for a visit to the employment tribunal. Poorly judged comments on public internet forums can be slanderous or breach confidentiality guidelines.	Nearly four in ten of our respondents found it challenging to address these legal risks. On the other hand, companies with effective web filtering and monitoring can provide reassurance and reduce risks. MessageLabs Security SafeGuard can prevent access to inappropriate websites and block specific types of downloads or access to online forums, chat and social networking sites.
Wasted bandwidth	67 percent of our respondents were concerned about the amount of expensive bandwidth wasted by non-work internet use. With the rise of social networking, streaming audio and video sites and TV-on-demand business, internet connections are under strain like never before. Our analysis suggests that 23 percent of a business's bandwidth is used for non-work internet access.[4] This represents a waste of money and it reduces the bandwidth available for legitimate work. The result is slower email, web browsing and VPN connections.	MessageLabs Security SafeGuard protects your company's bandwidth by stopping unwanted traffic before it even reaches your internet connection. Based on sophisticated policy controls, it blocks banned websites, downloads, email spam and media streams on our own systems before they reach your network. This preserves your bandwidth for real work. Because it also protects remote and home workers, it can preserve expensive wireless broadband connections and home worker's links back to the company network.
Unprotected mobile workers	Even if companies have in-house systems to monitor and control web access and to protect web users from malware, they often don't cover remote users working on laptopsand home workers operating outside the corporate firewall. This leaves a significant part of the workforce unprotected and this issue represented a serious management challenge for 42 percent of respondents.	MessageLabs Security SafeGuard extends web protection and filtering to remote users, including policy enforcement. It also ensures that remote users' online activities are tracked by the service's reporting tools.

[4]See MessageLabs "Bandwidth bandits" white paper 2010.

Threat	Why it matters	How to protect your business
Uncontrolled access to web applications	The internet offers a wide range of online applications, from web mail or social networking through to sophisticated business applications. Employees can use these to bypass corporate guidelines on security; for example, to access personal email or upload company data to services that are outside company control. This reduces the IT department's control over data and security. 42 percent of respondents worried about employee access to web mail or instant messaging applications. As the sophistication of online applications increases, this is going to become a significant problem.	Companies need to decide what kind of access they want to give employees. Some will want to block non-work sites completely. Others will want to allow access to some sites or within certain time limits. Also, increasingly, companies will allow employees access to approved online services, such as hosted CRM applications.

MessageLabs Security SafeGuard gives you granular control over which sites are allowed and which are denied. You can also limit access to personal sites during office hours or with time limits. |
| Malware | Websites are a growing security threat because so many of them contain malware. Symantec.cloud services blocked 4,998 malicious websites a day in February 2010.[5] This represents an increase of 198 percent since January. Four in ten of these sites and 13.3 percent of the viruses we discovered were new, which means that online criminals are changing their techniques rapidly to avoid detection.

As with any kind of malware, the consequences of infection are severe. Clear-up takes time, diverts IT resources and costs money. Infection renders confidential company information vulnerable and undermines the IT department's efforts to provide assurance to the board about security. | The majority of our respondents (92 percent) felt that they were able to protect their business against malware; although 40 percent found it a serious management challenge.

That said, nearly half of the IT managers we surveyed recently said that they knew a company that had suffered a virus attack.[6] Clearly, some companies may have a false sense of security about their protection.

Because of the growing sophistication and rapid evolution of website-based malware, it is essential to have protection that goes beyond signature detection. Symantec MessageLabs Web Security.cloud offers a combination of signature scanning and advanced heuristic protection using proprietary Skeptic™ technology. It is backed by 19 patents granted or pending and a team of 70 anti-malware experts. |
| Protecting multiple sites | Among respondents with 500 or more employees – the companies most likely to have several offices – 76 percent said that protecting multiple sites was a major issue. For this group, it was in fact the biggest issue. This is primarily because it is challenging to protect a single site. You need anti-malware, web filtering and monitoring software and all the support needed to keep it up to date. But with multiple sites, all this hardware and administrative overhead is multiplied. | Because MessageLabs Security SafeGuard is an internet-based hosted service, it can protect many offices just as easily as it can protect one. Similarly, it doesn't care how many email servers you have. Unlike in-house solutions, you don't have to pay an upfront capital cost for hardware and software followed by an unpredictable ongoing maintenance cost. Instead, you pay a fixed fee per user. |

[5]MessageLabs Intelligence as of 23 March 2010: http://www.messagelabs.co.uk/intelligence.aspx
[6]MessageLabs research for "Converged Threats, Integrated Defences" white paper 2009. 47 percent of respondents said that another business that they knew well had suffered a malware attack.

Symantec MessageLabs Security Safeguard.cloud

The number of threats and their diversity may be the biggest problem of all. Historically, companies have identified a problem and either accepted the risk or bought a point solution to address it. Many corporate data centers have separate servers for spam filtering, malware protection, web filtering and so on. Each new box adds to the IT department's cost base and management overhead. They rarely play well with one another and each one requires a different set of skills to maintain.

In contrast, Security SafeGuard.cloud provides an integrated system where each piece – web filtering and security, email protection and so on – complements the others and shares the same management portal and reporting capabilities. There is no hardware or software to buy. No new boxes for the data center or server room. Just a fixed, predictable per-employee fee.

When IT managers are asked to protect company data, prevent virus infections, support HR policies and guarantee bandwidth and service levels, Security SafeGuard.cloud is an essential tool.

To understand more about Security Safeguard.cloud, visit our website or request a free trial at
https://www.messagelabs.com/trial

More Information

AMERICAS

UNITED STATES

512 Seventh Avenue

6th Floor

New York, NY 10018

USA

Toll-free +1 866 460 0000

CANADA

170 University Avenue

Toronto, ON M5H 3B3

Canada

Toll-free :1 866 460 0000

EUROPE

HEADQUARTERS

1270 Lansdowne Court

Gloucester Business Park

Gloucester, GL3 4AB

United Kingdom

Tel +44 (0) 1452 627 627

Fax +44 (0) 1452 627 628

Freephone 0800 917 7733

LONDON

3rd Floor

40 Whitfield Street

London, W1T 2RH

United Kingdom

Tel +44 (0) 203 009 6500

Fax +44 (0) 203 009 6552

Support +44 (0) 1452 627 766

NETHERLANDS

WTC Amsterdam

Zuidplein 36/H-Tower

NL-1077 XV

Amsterdam

Netherlands

Tel +31 (0) 20 799 7929

Fax +31 (0) 20 799 7801

BELGIUM/LUXEMBOURG

Symantec Belgium

Astrid Business Center

Is. Meyskensstraat 224

1780 Wemmel,

Belgium

Tel: +32 2 531 11 40

Fax: +32 531 11 41

DACH

Humboldtstrasse 6

Gewerbegebiet Dornach

85609 Aschheim

Deutschland

Tel +49 (0) 89 94320 120

Support :+44 (0)870 850 3014

NORDICS

St. Kongensgade 128

1264 Copenhagen K

Danmark

Tel +45 33 32 37 18

Fax +45 33 32 37 06

Support +44 (0)870 850 3014

ASIA PACIFIC

HONG KONG

Room 3006, Central Plaza

18 Harbour Road

Tower II

Wanchai

Hong Kong

Main: +852 2528 6206

Fax: +852 2526 2646

Support: + 852 6902 1130

AUSTRALIA

Level 13

207 Kent Street,

Sydney NSW 2000

Main: +61 2 8220 7000

Fax: +61 2 8220 7075

Support: 1 800 088 099

SINGAPORE

6 Temasek Boulevard

#11-01 Suntec Tower 4

Singapore 038986

Main: +65 6333 6366

Fax: +65 6235 8885

Support: 800 120 4415

JAPAN

Akasaka Intercity

1-11-44 Akasaka

Minato-ku, Tokyo 107-0052

Main: + 81 3 5114 4540

Fax: + 81 3 5114 4020

Support: + 852 6902 1130

About Symantec.cloud

Symantec.cloud uses the power of cloud computing to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging. Building on the foundation of MessageLabs market leading software-as-a-service (SaaS) offerings and proven Symantec technologies, Symantec.cloud provides essential protection while virtually eliminating the need to manage hardware and software on site.

More than ten million end users at more than 31,000 organizations ranging from small businesses to the Fortune 500 use Symantec.cloud to secure and manage information stored on endpoints and delivered via email, Web, and instant messaging.

Symantec.cloud helps IT executives to protect information more completely, manage technology more effectively, and rapidly respond to the needs of their business.

For specific country offices and contact numbers, please visit our website.

Symantec.cloud North America
512 7th Ave.
6th Floor
New York, NY 10018 USA
1 (646) 519 8100
1 (866) 460 0000
www.MessageLabs.com