CLEARSWIFT™
Simplifying content security

15 Common Mistakes in Web Security

Enterprise vulnerabilities that invite attack

CLEARSWIFT™
Simplifying content security

Introduction

How many mistakes are you making?

The web is an increasingly dangerous place – a limitless universe of information, services, diversions and perversions.

To most enterprises, it's also a priceless resource. Before you question its value, try turning it off for a day. That screeching sound is your business grinding to a halt (accompanied by thousands of employees baying for blood).

The web may be a critical business tool, but it's also a major threat to your network resources, your reputation and your business. Web-borne viruses, spyware, malicious code, data leaks, identity theft, pornography and illegal files are just as happy landing on a corporate PC as on a domestic one.

Chances are, you're already doing a pretty good job stopping spam and viruses that arrive as email. But few enterprises are as rigorous in their web defense.

This booklet is about helping you defend your organization against web threats and about making your life easier in the process. It identifies fifteen of the most common web security mistakes we see every day in enterprises of every size – reflecting over twenty years of experience in helping tens of thousands of companies secure their Internet traffic – both email and web.

Section I deals with the principles of Enterprise Content Governance and the mistakes many companies make in setting and enforcing policy.

Section II gets more specific, summarizing the most common mistakes made by network administrators and identifying some of the consequences of these lapses.

The list is not exhaustive, but it should be enlightening. As obvious as some of the recommendations may seem, we know of very few organizations that follow them all.

The goal of the booklet is simple: to help network administrators and other IT professionals avoid the most common security mistakes so we can all use the web with confidence – while making life a lot more difficult for the bad guys.

Section I: Good Governance

Mistake 1

Not having a written web security policy.

Amazingly, many organizations still don't have any kind of formal web policy. They may have a loose set of rules, but nothing written down, regularly updated and distributed to all staff. That means employees have no idea what's acceptable and what's unacceptable behavior when they open a browser (and companies have little recourse when something goes horribly wrong).

The downside risks are well documented: the business suffers from lost confidential data, legal prosecution and reputation damage – without having a leg to stand on in its defense. Fairly or not, IT departments are often blamed for not detecting and stopping the breach.

An effective web policy does several important things:

- Prevents breaches instead of just reacting to them
- Allows the business to take action against offenders
- Helps establish due diligence in preventing web abuse
- Clarifies the things that the IT department is expected to defend against

Web security calls for three simple steps: Create a clear, sensible policy; Get commitment from everyone in the business; Enforce the policy diligently and publicly. Which brings us to the next common mistake…

Only 63% of businesses have an acceptable use policy for the Internet.

DTI Information Security Breaches Survey 2006

CLEARSWIFT™
Simplifying content security

Mistake 2

Failing to enforce your web security policy.

Just having a policy does not ensure that everyone will adhere to it. It's essential to actively police the rules – and to be seen to be doing so.

The risks:

- A policy without 'teeth' fails as a deterrent to web abuse
- An un-enforced policy will undermine efforts to punish web abusers and may not stand up in court

Use technology to back up your policy, and let all employees know that you're doing it. Preventing breaches is far better than simply catching culprits after the fact.

Filtering all web traffic as it enters and leaves the network is the only way to actively enforce your web security policy and is an essential element in Enterprise Content Governance.

The good news? It's easy to do, if you've got the right security solutions in place.

MIMEsweeper products proactively prevent policy breaches rather than simply reacting to them after the fact. You can set the thresholds and alerts so that the right manager or administrator can respond to web abuse through education and training rather than disciplinary procedures.

Policy Vacuum

A large UK retailer dismissed an employee for damaging its reputation on his blog. His defense? The employer had ***'no clear policy'*** on blogging.

CLEARSWIFT™
Simplifying content security

Mistake 3

Applying a blanket policy to all users.

Different people and departments have different needs and specific ways of using the web. An effective security policy takes into account the way you do business.

The risks

- A broad policy that makes sense for most employees may be crippling to others. This gives the IT department an undeserved reputation for obstructing business instead of enabling it
- Similarly, a lenient policy based on the needs of a small minority of users may leave massive loopholes open to the rest of the staff

An effective web policy can be extremely granular, making it clear, for instance, that only the music department is allowed to download MP3 files; or that webmail is forbidden in the R&D department but allowed in Sales & Marketing.

A detailed policy may seem harder to communicate, but in reality, it's the only way to get buy-in and to allow every user to get on with their jobs without putting themselves, or the business, at risk.

If users see that a policy makes sense – and that it's flexible enough to allow for different needs – they're more likely to respect it.

MIMEsweeper web security products filter all web traffic in both directions to identify and block breaches of your policy. Set policy in as granular a way as you like – down to the individual user, if necessary – and monitor compliance in real time.

CLEARSWIFT™
Simplifying content security

Mistake 4

Making the IT department the sole ‘owner’ of policy enforcement.

Web security is not just an IT issue. But too many companies leave the enforcement to the IT department alone.

This can put administrators in the position of having to judge what is acceptable and unacceptable content or behavior, without having the information to support the judgment.

The risks

- Over-burdened administrators weaken web security
- IT people may miss serious breaches that concern other business managers

Your web security defenses should allow for roles-based management so that the right manager can make judgment calls on each type of breach. The Human Resources department may be best placed to evaluate employment-related issues, while the compliance officers will need to rule
on financial data leaks.

Without this federated approach, IT departments can be perceived either as ‘over-protecting’ the business and stifling the free flow of information or ‘under-protecting’ and allowing serious breaches to go un-blocked.

Enlisting the relevant management teams in the web security strategy increases the power of the defenses while significantly reducing the burden on the IT department.

MIMEsweeper web security products feature a unique roles-based management function that allows organizations to give responsibility for policy enforcement to the right manager, therefore reducing the burden placed on IT professionals.

Failing to Police Porn

A UK Government department was forced to discipline **227** members of staff for downloading pornographic images from the web. After only sixteen of these employees were fired, the media criticized the department's policy enforcement.

As one online journal reported, *"…any audit trail will be able to clearly discriminate between those who strayed to a website by mistake and never visited it again and those who repeatedly returned. The reporting capabilities of such systems can now build up a body of evidence that would support any decision to dismiss an employee for inappropriate use*."

Not regularly monitoring web activity.

This one seems too obvious to state, but it's amazing how many companies fail to implement even the most rudimentary web activity reports.

The risks

- Long-term web abuse goes un-noticed
- Regulators view the absence of reporting as a sign of less than serious compliance efforts
- If you don't understand 'normal' trends, you won't spot the abnormal activity that signals abuse

Monitoring web activity across your organization never fails to flag things you need to be aware of. The most basic things you need to see, broken down by user, department or location, include:

- **Web activity** – visited and blocked sites
- **Number of requests** – web sites and pages most commonly visited
- **Volume of data sent** – bandwidth usage
- **Files up and downloaded** – file types from where to whom
- **Spyware detected** – 'call homes' to known spyware sites identified by machine

Good reporting will let you spot the anomalies and take a step towards explaining them.

You might identify a particular PC that has been taken over by spyware and is broadcasting spam. Or spot an employee who is running an illegal video download business from company servers. Or track down the source of a major leak of confidential data.

Monitoring also lets you spot general trends in web usage so you can plan resources (such as storage or bandwidth) and tweak policies.

MIMEsweeper web security solutions always include rich, web-based reporting tools so you can keep an eye on web activity and nip problems in the bud. You can even set alerts to be issued when certain thresholds are approached.

Section II: Best-practice web security

Failing to defend against malicious code at the web gateway.

Desktop defenses alone aren't good enough anymore. You need to add a layer of protection at the web gateway, so you can stop spyware, viruses and all other malicious code before it hits your users' browser and then your network.

The same principle has been applied for years at the SMTP gateway for email, but the web gateway is often relatively undefended.

The risks

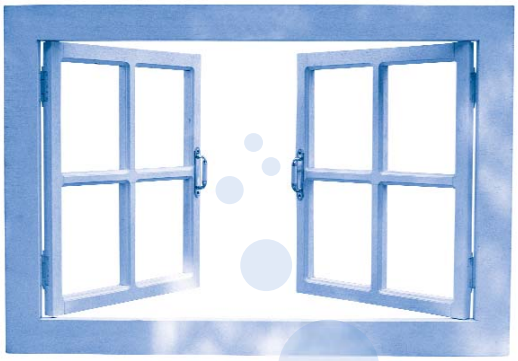
- Waiting for malware to hit the desktop multiplies the chances that it spreads before you can remove it
- Letting malicious content inside the firewall increases the cost of security

Best practice calls for different anti-virus and anti-spyware filters at the gateway and desktop. So if one vendor hasn't recognized the malware yet, the other might.

This defensive depth is essential to safe web use – and actually makes the IT department's life easier, not harder.

MIMEsweeper web security software and appliances bring enterprise-class web security to the gateway – your first and most important line of defense. Our software works with any third-party anti-virus or anti-spyware engine, while our appliance integrates best-of-breed anti-virus and anti-spyware in one solution.

CLEARSWIFT™
Simplifying content security



Mistake 7

Leaving the Zero-day window wide open.

The best anti-virus and anti-spyware software are great at identifying known malware. But a lot of damage can be done by new viruses and spyware before a profile can be captured and distributed to your filters.

The risks

- New viruses and spyware can spread throughout your network in less than an hour
- By the time a patch is installed, the damage is done

Content filtering offers an essential defense against zero-day attacks by identifying and blocking traffic that looks, smells and behaves like a virus or spyware script.

As well as offering this zero-day protection, a good content filter will also detect a wide range of abusive behavior and undesirable content such as financial spreadsheets being web-mailed out from the accounts department before the quarterly results announcement.

The zero-day protection offered by content filtering is one of the easier and most effective defenses you can deploy.

MIMEsweeper invented content filtering and continues to lead the market in technology and in deployments. Our deep content analysis closes the zero-day window, catching malicious code even before a virus or spyware profile can be issued.

CLEARSWIFT™
Simplifying content security

Mistake 8

Not stopping spyware call-homes.

When spyware installs itself on one of your computers, its first job is to call home, report on its success and receive further instructions.

Each of these ‘call-homes’ leaves a distinctive signature. If you’re looking for them, you can stop them, rendering the spyware ineffective.

The risks

- Spyware that successfully calls home is instantly activated and the problems begin
- If an employee brings spyware into the network from home, it may invalidate your outsourcing agreements, leaving you open to compensation payments

Even if an employee brings spyware into work on a laptop, the call-home can be caught before the spyware activates – but only if you’re looking for it.

Believe us, spyware writers hate this feature. Which is one reason we love it.

The MIMEsweeper Web Appliance uses Aluria spyware profiles to stop spyware at the gateway. Call-homes are blocked using Aluria’s database of known spyware sites and MIMEsweeper content filtering technology.

Letting employees download executables and shareware.

Very few employees have a legitimate need to download executable files. Your policy should bar them for all but the most educated users (the IT department may make legitimate use of .exe files and will understand the concept of trusted sources).

Spyware and adware often comes invisibly bundled in with even the most useful shareware programs. Few users read the terms & conditions that might include an agreement to install adware.

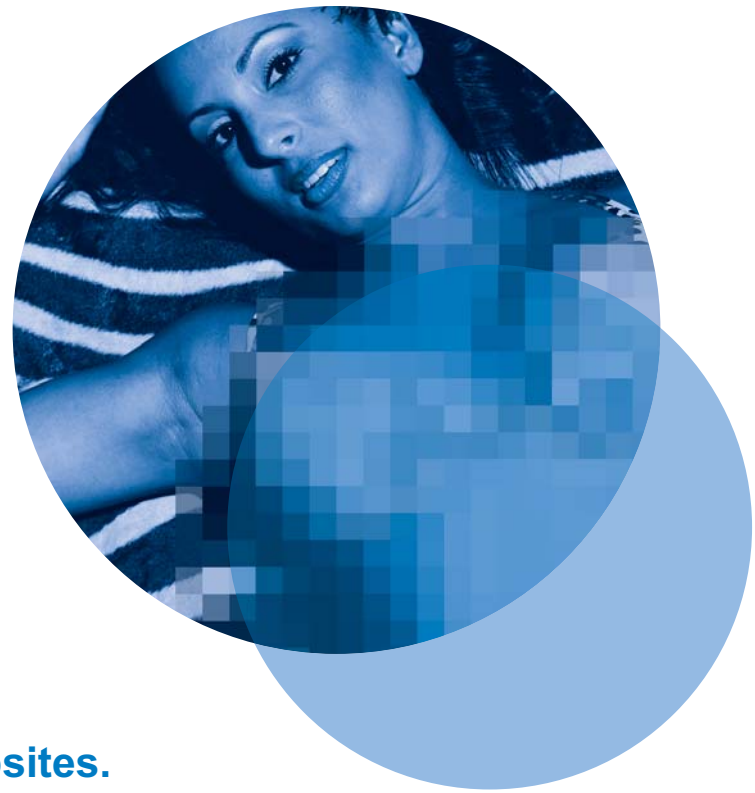
The risks

- A seemingly benign piece of shareware can bring down a network… or a brand reputation
- Spyware often resets browser security settings to minimum levels putting users at risk of further damage

Free software is tempting. Remove the temptation by blocking executables and shareware in your policy and in your web filter. You'll see a noticeable reduction in spyware and adware.

Granular policy management lets you specify who gets to download what – and who receives an alert when it happens. No policy management is more granular than MIMEsweeper's.

CLEARSWIFT™
Simplifying content security



Mistake 10

Not blocking access to dubious websites.

You may decide to allow access to non-business websites, such as shopping, news or entertainment sites. But do you really want employees accessing sites with child pornography, hate speech, hacking tips or sites know to be crawling with spyware?

Surfing from a company computer is not just a personal issue anymore. It can have serious consequences for your network and your reputation.

The risks

- Headlines about staff downloading pornography can set your reputation back years
- Illegal file downloads could make your company liable to prosecution

An effective URL Filter that allows you to block specific sites as well as entire categories is essential.

Once in place, such a filter stands guard at your web gateway, stopping policy breaches with no human intervention.

MIMEsweeper web security solutions include one of the world's most comprehensive URL Filters, cataloguing over 18 million URLs and 2 billion web pages into 40 distinct categories (such as pornography, gambling, auctions, webmail, etc).

A Critical Leak

A US software company hit the news when source code and key design documents were stolen from its R&D centre in India.

A new employee had used a web-mail account to upload the data. Development at the center was temporarily stopped as management tried to track down the code and stop it spreading. But the news story had already run all around the world.

Relying on URL blocking alone.

URL Blocking is an important part of any web security strategy – but for many companies it's the only web defense in place.

The URL filter may stop employees from accessing some sites that are known to contain spyware or viruses, but it can't block them all – even if you set it at the strictest possible level (which few enterprises are happy to do).

The risks

- Spyware and viruses still find their way in to your network
- Confidential data leaks leave the network untouched

The good news: it's easy to integrate URL filtering with the other essential web security processes with no significant latencies or administrative burdens.

MIMEsweeper Web Appliance integrates URL Filtering, Anti-Virus, Anti-Spyware and Content Filtering in a single, plug 'n' play solution that updates itself.

CLEARSWIFT™
Simplifying content security

Infected PC leaks nuclear secrets

In June, 2005, sensitive information about nuclear power plants in Japan was leaked over the internet from a virus-infected computer. The confidential reports were posted to a file-sharing site after an engineer's laptop was infected with a virus while working at home.

The lost data included photographs of the insides of nuclear power plants and the names and addresses of inspecting engineers.

Mistake 12

Only filtering inbound traffic.

A lot of nasties come from outside the organization. But outbound traffic can be just as hazardous to your health.

The risks

- Rogue employees can use webmail to send out confidential data, such as customer data, product designs or marketing plans
- Clueless users can bring spyware in to the office on laptops, then send it to your customers and partners
- Staff can use office resources to send out stolen MP3s, movies and pornography

Clearly, no web defense is complete unless it filters outbound traffic with the same vigilance as inbound. The trick is to automate this process to minimize human intervention and maximize security.

MIMEsweeper offers comprehensive, bi-directional web security, applying anti-virus, anti-spyware, URL blocking and content filtering to outbound traffic as well as inbound.

Failing to break down ‘container’ file types.

Some file types routinely contain other files – including malware. Defenses that don’t break down these containers and analyze the contents aren’t defenses at all.

Popular office files including spreadsheets, word processing and presentation files are all vulnerable to ‘fuzzing’ – the attacker supplies data designed to make the application crash, then exploits the next instruction point that remains in memory (an executable kicks in as soon as the application fails, and voilà: you’re infected).

The risks

- Crashed networks, unavailable applications frustrated users and customers

The only solution: decompose all container file types to scan for deeply embedded malware.

Of course, you can’t do this by hand. You need an automated solution that decomposes every message to its smallest parts, analyzes each one and takes the appropriate action.

A lot of hackers assume you won’t go this far to defend your network. But they don’t know how easy it can be.

MIMEsweeper technology uses deep, recursive analysis to break down all container files into their constituent parts, then analyze each one independently.

CLEARSWIFT™
Simplifying content security

Mistake 14

Believing the stated file type.

Attackers often hide themselves by simply misstating the file type extension. Sounds about as obvious as throwing a sheet over your head, but it does defeat basic defenses with alarming frequency.

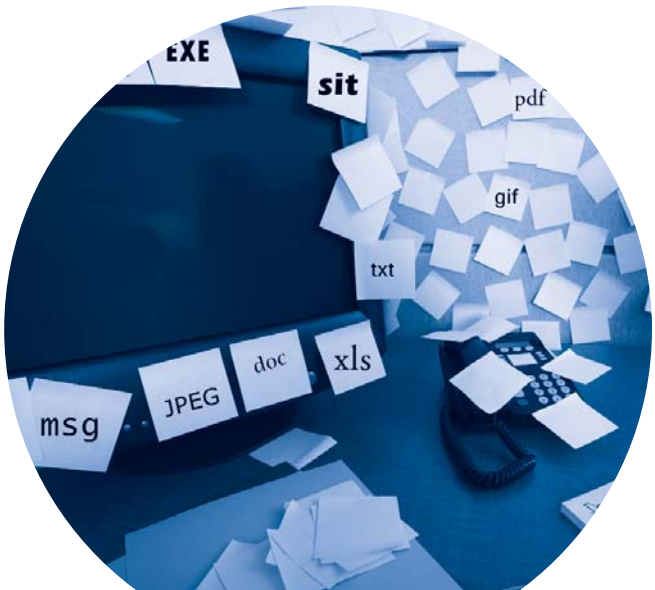
The risks

- One of the simplest ways of all to smuggle viruses, spyware and Trojans into the network

Rule of thumb: just because it says '.txt' at the end of the file name, doesn't mean it's really text.

In web security, it pays to be suspicious.

MIMEsweeper web security looks at the binary pattern, not just the file name, to identify the real file type. Does your gateway solution?



Over-burdening your administrators.

A web security solution that asks too much of its administrators is asking for trouble. Deploying a range of point solutions for each threat or different defenses at every gateway makes deploying, updating, managing and monitoring a nightmare.

The risks

- Over-complicated or poorly integrated web security wastes time and resources
- Security that isn't easy to manage gets updated less often, weakening security

Roles-based management further reduces the burden on IT by letting the right managers anywhere in the business play a role in enforcing policy in their domain.

Clearswift simplifies web security with software and appliances that are easy to install, maintain, update and manage.

Our web security appliances pre-integrate all of the key web defenses – anti-virus, anti-spyware, URL blocking and content filtering – in a single solution. And our software integrates easily with your own chosen solutions to create a single system.

Updates are automated and multi-box support makes central policy management and reporting easy, while roles-based management shares the burden beyond the IT department.

CLEARSWIFT™
Simplifying content security

The Next Fifteen Mistakes

The challenges of Enterprise Content Governance.

Since we can't live without the web, we need to find new ways of living with it. Ways that allow your people to do their jobs without opening up your networks, servers and PCs to a Pandora's Box of spyware, viruses, malicious code, data leaks, identity theft, pornography and stolen James Bond films.

It's all part of a broader discipline that we call Enterprise Content Governance, a strategic response to the inbound, outbound and internal threats carried by email and web traffic.

Proper content governance is getting much more difficult. We've come a long way from the pimply hacker, breaking into networks for fun. Today, spyware alone is a multi-billion dollar industry that invests huge resources to stay ahead of new defenses.

The web security mistakes listed here are only a small subset of all the potential vulnerabilities that make life easier for the bad guys and a lot harder for the rest of us.

Comprehensive web security boils down to this:

- **Establish and promote a practical web use policy** – that reflects the way you do business.
- **Enforce that policy with the right technology** – that filters all traffic, for all threats, at all gateways, in all directions.
- **Keep it simple** – by integrating defenses, automating administration and streamlining reporting.

Clearswift pioneered web security back when the web was new. We've seen every kind of attack and defense in every kind of environment, from the smallest business to the largest global enterprise.

What we've learned is built into our solutions. And we never stop learning (because the bad guys never stop innovating).

Talk to us about simplifying your web security without compromising. Or visit www.clearswift.com to see an introduction to our web security products.

About Clearswift

Clearswift simplifies content security.

Our products help organizations enforce best-practice email and web use, ensuring all traffic complies with internal policy and external regulations.

Our range of content filtering solutions makes it easy to deploy, manage and maintain no-compromise email and web security for both inbound and outbound traffic.

Clearswift is the only vendor to offer comprehensive, policy-based content security in all three deployment methods: as software, as an appliance and as a managed service.

All three platforms are designed to take the hassle out of securing internet traffic, with a clear, intuitive management interface; automatic, 'zero-touch' updates; powerful reporting and common-sense policy management.

Twenty years of experience across 17,000 organizations has helped us raise security standards while simplifying security management at the same time.

We've helped many of the world's most successful organizations use the internet with confidence and are committed to staying ahead of the market and helping our customers defend against all emerging threats.

Contact Clearswift

United States
100 Marine Parkway, Suite 550
Redwood City, CA 94065
Tel: +1 800 982 6109 | Fax: +1 888-888-6884

United Kingdom
1310 Waterside, Arlington Business Park, Theale,
Reading, Berkshire, RG7 4SA
Tel: +44 (0) 11 8903 8903 | Fax: +44 (0) 11 8903 9000

Spain
Cerro de los Gamos 1, Edif. 1
28224 Pozuelo de Alarcón, Madrid
Tel: +34 91 7901219 / +34 91 7901220 | Fax: +34 91 7901112

Germany
Amsinckstrasse 67, 20097 Hamburg
Tel: +49 40 23 999 0 | Fax: +49 40 23 999 100

Australia
Ground Floor, 165 Walker Street, North Sydney,
New South Wales, 2060
Tel : +61 2 9424 1200 | Fax : +61 2 9424 1201

Japan
Hanai Bldg. 7F, 1-2-9, Shiba Kouen Minato-ku
Tokyo 105-0011
Tel : +81 (3) 5777 2248 | Fax : +81 (3) 5777 2249