Open Source Email Security Solutions: 10 Questions

A strategic resource for IT decision-makers in small and medium size businesses

A MailSite, Inc. White Paper

June 2008

mailsite® FUSION

INTRODUCTION

Email security: a strategic issue

Email security has become a strategic issue for IT executives. The risks of making a mistake are business critical. The costs of making a wrong decision are measured not in terms of wasted IT budgets, but in terms of lost revenues, fraud, the leaking of confidential information, and, increasingly, lawsuits. Virus infections - 99% of which are distributed by email - can cause your business to grind to a halt for hours or days, and they can use your machines to self-propagate and spread throughout the internet, including to your customers and suppliers.

In addition, email security attacks are increasing in sophistication. An example is the increase in the number of attacks by "spyruses" - self-propagating viruses that distribute spyware programs - which aim to harvest confidential information such as user names and passwords.

Build or Buy?

One of the key considerations when making an email security purchasing decision is whether to "build" - to build a custom solution using one or more open source software programs - or to "buy" - to invest in a packaged solution from a commercial vendor.

Most commercial vs. open source debates focus on the Windows vs. Linux issue. In the context of email security, however, the core issue is not one of operating system preference, it is one of whether to entrust the ongoing security of your email system to the open source community or to a commercial vendor.

Aim of this paper

This paper aims to provide a checklist of risk management questions designed to help IT executives faced with a "build vs. buy" email security purchasing decision. It does not aim to offer any answers, but rather to highlight the key issues that should be addressed during the process. The answers to the questions will depend amongst other things on each organization's culture, skills set, core competencies, strategic goals and cash flow.

10 QUESTIONS

1. Do you need to review your build vs. buy culture?

As the technology market matures, the number of organizations that have a cultural preference for open source or commercial solutions is decreasing. It has become good practice to base each purchasing decision on its own merits, rather than on how things have been done previously.

If your organization still has a cultural preference, what is the basis for that preference? Is it based on an individual's personal preference? If it is based on an ad-hoc, qualitative risk assessment, is it still valid?

Most small and medium size businesses will probably not use formal risk assessment methodologies. However a regular informal review of the premises behind past build vs. buy decisions will help to prevent old habits from becoming bad policy.

2. Is this the best use of your in-house resources?

Building an open source solution will divert more resources away from other projects than a commercial solution, which will result in an "opportunity cost". The opportunity cost - the cost of what has to be given up as a result of the decision - is the total value of other projects that will be cancelled or delayed.

The size of the opportunity cost will also depend on the strategic importance of the projects being cancelled or delayed. For example, the cost of delaying the launch of a new webstore will depend on the impact the new webstore is expected to have on revenue generation, customer churn, cost of sale, or market share.

The opportunity cost of diverting internal resources is an important element of the decision making process that is often overlooked.

3. Is open source or commercial more reliable?

In the context of email, the prime security issue is not necessarily one of which operating system is the most secure: it is about reliability of updates. While your administrator is responsible for ensuring the reliability of internal systems, and for ensuring that the latest patches have been applied to an open source solution, they cannot be held accountable if a third party server fails to release the updates in time to prevent infection.

Even though commercial vendors usually have limited liability clauses, it is core to their business activity to ensure that update services are timely and reliable, as any failure will result in loss of revenues as customers move elsewhere.

4. Is your cost analysis comprehensive?

For any organization faced with an open source vs. commercial choice the total cost of the project will be a key factor, if not ***the*** key factor, in the decision making process.

Open source solutions do not incur license, maintenance and update fees, but they are not "free". Compared with commercial solutions, they require more resources to build, install, configure, update the software programs, and maintain the threat definition data. Building an open source solution also requires a time investment in documenting, testing and bug-fixing each iteration of the solution.

It has been argued that because most open source software runs on Linux, which is a more secure solution than Windows, it will require fewer resources to maintain the security of the servers on which the solutions are deployed. However the relative security of the two operating systems remains a moot point, and an in-depth analysis by the Yankee Group in 2004 concluded that businesses will expend as much time, money and resources securing their Linux systems and servers as they now devote to Windows security.

Other additional costs of an open source solution that can easily be overlooked include:

- More support staff: according to a 2004 Yankee Group survey Linux requires between 25% and 40% more support specialists than Windows.
- Pay differentials: you need a higher level of expertise to run open source solutions, which costs more. Expect a pay differential of between 15% and 30%.

5. Is this the best strategic fit for your company?

The implications of a decision in favor of an open source or commercial solution should be mapped against broader business pressures and strategic goals.

A decision to implement an open source solution involves a long-term commitment to an in-house development resource. If maintaining this resource for internal projects is not a strategic goal for your organization then there is a risk that development resources will be cut or redeployed to higher priority projects.

On the other hand, commercial solutions can risk a lock-in to a single vendor, resulting in escalating license and support fees. Single vendor lock-ins can be avoided by using a standards-based solution that is easily replaced and which can more readily adjust to changing infrastructure requirements.

6. Is there a satisfactory disaster recovery strategy?

Even the most comprehensive and sophisticated email security solutions cannot guarantee 100% protection. If an infection does occur, or if data security becomes compromised, the key issue is speed of recovery.

A successful disaster recovery process will hinge on the availability of the specific skills required to clean and disinfect your network, to identify the cause of the problem, and to fix it.

The skill set and skill level needed to implement disaster recovery will be higher for an open source solution than for a commercial one. This has cost implications. It can also have a serious impact on the speed of recovery if an open source solution can only be debugged and patched by the highly skilled engineers that built it, and they are not available or no longer with the company.

7. Is there adequate provision for maintenance & updates?

Supporters of open source solutions have set up rule set and spam definition update services, but they deliver less frequently than commercial solutions and there is no accountability for service failure.

This is a key element of the value proposition for commercial vendors, the best of which will have teams of experts on 24 x 7 schedules working on identifying new threats, testing solutions in development labs, and ensuring their timely delivery to customers.

Some commercial vendors also provide software updates via their automated delivery service, which enables them to be installed with no administrator intervention. This provides a significant saving in time and money over open source solutions, as well as being a faster, more effective way of ensuring that defenses are kept up to date.

8. Are deployment and update time estimates accurate?

Thanks to the increasing number of tools that have been developed by the open source community, deploying an open source solution has become much faster. It will still take far longer to deploy than the best commercial solutions which have multiple security modules integrated in one package.

In addition, quality commercial packages will include a range of documented, standards-based APIs to facilitate rapid integration with existing infrastructures.

As a result, deployment and update timelines for commercial solutions should be significantly shorter than open source.

9. Is there adequate provision for creating and maintaining the documentation?

One of the key challenges for an in-house solution is how to ensure that software documentation is created and maintained on an ongoing basis. Even if you set out with the best of intentions, all too often the commercial reality of resource conflicts

lead to the ongoing documentation of an in-house solution being given too low a priority, as a result of which it is neglected.

A good commercial solution will have detailed administration manuals that are regularly updated by vendors. In addition, a good vendor will support the documentation with live support services, technical papers, and online knowledge bases that are updated regularly.

What might be a webmaster's email security masterpiece could quickly become an expensive liability if the authors cease to be employees, or if they are on leave.

10. Will this solution help differentiate you from your competitors?

If your organization is in the finance, internet service provider or web hosting sectors, you will know that email security is a strategic differentiator. Being able to secure and protect your client's communications and your client's data is a core business requirement.

As we have seen recently, security threats can be distributed globally in seconds, and within a few hours the same threat can be redistributed having morphed into a dozen different variations each with a different signature. Protecting against these threats requires the best you can get for your budget.

It used to be said that organizations should "buy for parity, build for advantage". This maxim does not ring true, however, if your home-built open source solution system does not block new virus updates as effectively as a commercial solution!

CHECKLIST

10 questions to ask yourself before choosing an open source email security solution

		YES / NO
1	Do you need to review your build vs. buy culture?	
2	Is this the best use of your in-house resources?	
3	Is open source or commercial more reliable?	
4	Is your cost analysis comprehensive?	
5	Is this the best strategic fit for your company?	
6	Is there a satisfactory disaster recovery strategy?	
7	Is there adequate provision for maintenance & updates?	
8	Are deployment and update time estimates accurate?	
9	Is there adequate provision for creating and maintaining the documentation?	
10	Will this solution help differentiate you from your competitors?	

http://www.mailsite.com/products/av/mailsite-anti-virus-filter.asp

About MailSite Software Incorporated

MailSite Software Incorporated develops a low cost alternative to Microsoft Exchange for carriers, telcos, service providers, enterprises and businesses worldwide. MailSite, Inc. was established in 1995 under the name Rockliffe and is based in California's Silicon Valley with European headquarters in the UK. MailSite, Inc has more than 2,000 customers hosting more than 15 million mailboxes worldwide. These include service providers such as Verizon, eChalk, NetOne and WestNet, and enterprises such as Teleflora, Encyclopædia Britannica, and MediaNews Group. MailSite partners include HP, Qualcomm, J2, Cegedim Rx, Rockwell Collins, Kaspersky and Mailshell.

MailSite Professional Services

MailSite Professional Services cover remote and onsite assistance with performance tuning, migrations, integrations, upgrades, email security audits, training, and custom software development. To discuss your requirements and arrange for a quote please contact **sales@mailsite.com**.

www.mailsite.com